CANTIERI DELLA PA DIGITALE

SICUREZZA DIGITALE | REPORT 2018

FPA

DIGITAL360

La redazione del report 2018 del Cantiere Sicurezza digitale è stata coordinata da Andrea Ivan Baldassarre, con la supervisione scientifica di Alessio Pennasilico.
Il documento costituisce il risultato finale del lavoro collaborativo **tra tutti i protagonisti del Cantiere** svolto nel corso dell'anno.
Il focus sul *fattore umano e sicurezza dell'end point* è stato curato insieme da un gruppo di lavoro composto (in odine rigorosamente alfabetico) da: Antonio Manduca (Enea), Carlo Bedetti (Ministero dell'interno), Carlo Fantini (Ministero dell'interno), Davide Bigoni (Samsung), Domenico Cuoccio (InnovaPuglia), Enzo Veiluva (CSI Piemonte), Gemma De Angelis (Agenzia del Demanio), Giancarlo Buzzanca (Ministeri per i Beni e le Attività Culturali), Gianpaolo Araco (Senato della Repubblica), Giovanni Mellini (ENAV), Giuseppe Arrabito (Sapienza Università di Roma), Leandro Gelasi (Corte dei conti), Luca Mairani (ForcePoint), Massimiliano Chiardoni (Sogin), Matteo Rigoni (Samsung), Paolo De Carlo (Aizoon), Paolo Foschi (ForcePoint), Pasquale Fedele (ENEA), Pierluigi Sartori (Informatica Trentina), Raffaele Visciano (Ministero dell'Economia e delle Finanze), Roberta Lotti (Ministero dell'Economia e delle Finanze), Roberto Guadagni (ENEA), Rosario Riccio (Ministero dell'istruzione, dell'università e della ricerca), Stefano Plantemoli (Ministero dell'interno)
Il focus sulla *sicurezza applicativa* è stato curato insieme da un gruppo di lavoro composto (in odine rigorosamente alfabetico) da: *Marco Bessi (Cast Software), Giancarlo Cecchetti (Umbria Digitale), Massimo Crubellati (Cast Software), Domenico Cuoccio (InnovaPuglia), Paolo De Carlo (Aizoon) Marcello Di Monte (Ministero delle Difesa), Paolo Foschi (Forcepoint), Stefano Giannandrea (Lepida), Diego Mezzina (Insiel), Rosario Riccio (MIUR), Marco Romoli (Cast Software), Ettore Sala (Laziocrea), Michele Slocovich (Cast Software), Maurizio Trapanese (AIFA), Luca Tricca (Arma dei Carabinieri), Enzo Veiluva (CSI Piemonte)*

CANTIERI DELLA PA DIGITALE
Cantiere Sicurezza digitale - Report 2018 - Edizioni ForumPA - ISBN: 9788897169604

Finito di impaginare: febbraio 2019
con il contributo di:

SICUREZZA DIGITALE | REPORT 2018

INDICE

L'INIZIATIVA CANTIERE DELLA PA 6
INTRODUZIONE 8

FATTORE UMANO E SICUREZZA DEGLI END POINT 11
1. INTRODUZIONE **11**
KEY TAGS: OBIETTIVI, APPROCCIO METODOLOGICO, I RISCHI DI ESPOSIZIONE, IMPORTANZA DELLA MESSA A FATTOR COMUNE
2. LA SENSIBILIZZAZIONE COME FATTORE ABILITANTE ALLA CONSAPEVOLEZZA DEL RISCHIO CYBER **13**
KEY TAGS: NORMATIVA, FORMAZIONE, PRIORITÀ, CONSAPEVOLEZZA
3. LA DETERMINAZIONE DELLE LINEE GUIDA "ORGANIZZATIVE E COMPORTAMENTALI": CANALIZZARE IL MODUS OPERANDI **18**
KEY TAGS: CATEGORIZZAZIONE DELLE INFORMAZIONI, COMPORTAMENTI, PROCEDURE E REGOLE
4. LA CONDIVISIONE DELLE COMPETENZE: LA FIGURA DEL FOCAL POINT **20**
KEY TAGS: ES. DI APPLICAZIONE, IL RUOLO DEL FACILITATORE O DEL MASTER
5. IL PERCORSO PER EDUCAZIONE CYBER: LA FORMAZIONE DAL LIVELLO DECISIONALE ALL'OPERATIVO - SUGGERIMENTI PRATICI **21**
KEY TAGS: ANALIS DEI PERCORSI, DEFINIZIONE DEI TARGET, VERIFICA DEI RISULTATI
6. I PUNTI CARDINE DA PRESIDIARE NELLA DIFESA DELL'END POINT **23**
KEY TAGS: AUTENTICAZIONE, PROTEZIONE DELLA MAIL, PROTEZIONE DELLA NAVIGAZIONE, ACCESSO AI DATI, CIFRATURA DELLE INFORMAZIONI, ANALISI COMPORTAMENTALE DEI SISTEMI, IOT, MOBILE, AGGIORNAMENTO SISTEMI E BACKUP, CENTRALIZZAZIONE DI SERVIZI SU CLOUD, INDICATORI DI RISCONTRO
6.1 AUTENTICAZIONE **23**
6.2 PROTEZIONE DELLA MAIL **25**
6.3 PROTEZIONE DELLA NAVIGAZIONE **28**
6.4 LA CIFRATURA DELLE INFORMAZIONI **29**
6.5 ACCESSO AI DATI **31**
6.6 IL MONITORAGGIO DELLA RETE **32**
6.7 IL CONTROLLO DISPOSITIVI MOBILI **34**
6.8 L'ATTENZIONE AI SOCIAL **35**
7. CONCLUSIONI E MESSAGGIO ALLE ISTITUZIONI **36**

SICUREZZA APPLICATIVA 40

1. INTRODUZIONE **40**
LA SFIDA DELLA SICUREZZA APPLICATIVA
KEY TAGS: SICUREZZA DELLE APPLICAZIONI, SITUAZIONE ATTUALE E TREND, PRINCIPALI INIZIATIVE ED AZIONI
2. AMBIENTI APPLICATIVI E SICUREZZA **41**
KEY TAGS: APPLICAZIONI WEB, APPLICAZIONI MOBILE, IOT, CLOUD
3. LA DEFINIZIONE DEL CICLO DI SVILUPPO SICURO DEL SOFTWARE **45**
KEY TAGS: SSDLC, ANALISI, PROGETTAZIONE, SVILUPPO, COLLAUDO, HLD, CICLO DI VITA
4. LA DEFINIZIONE DEI REQUISITI E LA PROGETTAZIONE **48**

KEY TAGS: NORMATIVA, STANDARD, REQUISITI FUNZIONALI, REQUISITI NON FUNZIONALI

4.1 REQUISITI DI SICUREZZA FUNZIONALI **51**

4.2 REQUISITI DI SICUREZZA NON FUNZIONALI **52**

4.3 LINEE GUIDA PER IL SECURITY BY DESIGN **53**

5. LA SICUREZZA APPLICATIVA NELLE GARE E FORNITURE DELLA PA **55**

KEY TAGS: GARE, FORNITURE, CAPITOLATI

6. LE VERIFICHE, I TEST E LA MANUTENZIONE **57**

KEY TAGS: MANUTENZIONE, VULNERABILITÀ, TEST DI SICUREZZA, SAST, DAST, PT, VA, IAST, RASP

6.1 VERIFICHE DI SICUREZZA NELLA FASE DI SVILUPPO **61**

6.2 VERIFICHE DI SICUREZZA NELLA FASE DI TRANSITION **63**

6.3 VERIFICHE DI SICUREZZA NELLA FASE DI OPERATION **63**

7. UN ESEMPIO DI CHECKPOINT ORGANIZZATIVO **64**

KEY TAGS: VERIFICHE DI CONFORMITÀ, VA, PT, MINISTERO DELLA DIFESA

8. CONCLUSIONI E RACCOMANDAZIONI **66**

I PROTAGONISTI DEL CANTIERE **69**

L'INIZIATIVA CANTIERI DELLA PA

Lanciati nel 2016, i **Cantieri** sono i laboratori permanenti di FPA dedicati ai temi dell'innovazione digitale e organizzativa della PA italiana, nati con l'obiettivo di monitorare e supportare i percorsi di cambiamento nelle principali aree verticali e trasversali del processo di digitalizzazione della pubblica amministrazione, attraverso attività di analisi, networking, comunicazione e advocacy.

I Cantieri operano attraverso **tavoli di lavoro** che mirano ad individuare i principali ostacoli all'attuazione dell'innovazione, analizzando criticità comuni, opportunità e possibili soluzioni. Non un'indagine quantitativa, ma un'analisi basata sull'esperienza quotidiana dei protagonisti dell'innovazione, pubblici e privati. Tavoli di confronto che integrano soggetti, approcci epistemologici e interessi differenti in un ambiente realmente collaborativo, ma strutturato.

I Cantieri aggregano le community dei più autorevoli operatori pubblici e privati responsabili dell'attuazione dei processi di innovazione della PA italiana. Nell'arco dei primi 3 anni di vita dell'iniziativa sono stati attivati 10 tavoli di lavoro e realizzati 76 incontri a porte chiuse, che hanno visto la partecipazione di 430 operatori, tra cui 388 dirigenti pubblici provenienti da 95 differenti amministrazioni (30 centrali, 65 locali), 42 accademici ed esperti della *digital trasformation* e 37 imprese e grandi aziende sponsor.

I Cantieri rappresentano un ambiente collaborativo, aperto al **confronto "tra pari"** tra soggetti pubblici e privati. Ogni Cantiere è orientato alla costruzione di relazioni e partnership tra amministratori, dirigenti pubblici e rappresentanti delle aziende partner per contribuire al processo di attuazione della strategia digitale italiana. Gli incontri in presenza si alternano con momenti di riflessioni e confronto sulla piattaforma di knowledge sharing e community management di FPA, che ospita gli oltre 500 contenuti prodotti, tra documenti di approfondimento, dossier e post.

La comunicazione e l'attività di analisi e l'approfondimento dei temi trattati dai tavoli di lavoro viene ospitata sul sito cantieripadigitale.it, che raccoglie video interviste e contributi a firma dei protagonisti dei tavoli di lavoro, buone pratiche ed esperienze realizzate dalle amministrazioni e dalle aziende aderenti all'iniziativa.

I contenuti prodotti vengono veicolati attraverso una newsletter settimanale, rivolta a una community di oltre 70.000 operatori.

Al termine del ciclo annuale di attività, ogni Cantiere produce un report pubblico contenente una serie **raccomandazioni** rivolte ai decisori politici, ai responsabili delle diverse policy verticali e trasversali e a tutte le amministrazioni italiane, ad ogni livello. Le raccomandazioni possono consistere in indicazioni di metodo, punti di attenzione o in vere e proprie linee guida per facilitare l'effettiva attuazione dei processi di innovazione della PA.

INTRODUZIONE

a cura di Alessio L.R. Pennasilico, Information & Cyber Security Advisor Comitato Tecnico Scientifico di Clusit, Associazione Italiana per la sicurezza informatica.

Ritengo sia rilevante per chi sta per leggere questo documento conoscerne la genesi.
"Senza sicurezza non ci può essere trasformazione digitale. Vogliamo parlare di innovazione? Di sistema paese? Di tecnologie? Di metodologie? Di cultura? Vogliamo fare una proposta concreta. Dire qualcosa che possa essere utile a qualcuno!"
Ero a Roma, nei meravigliosi uffici di FPA, guardavo Castel Sant'Angelo dalla finestra. Da ore discutevamo di quali scenari avrebbe dovuto occuparsi quest'anno il "cantiere security".
Alla fine, si è, a mio parere, deciso di affrontare alcuni dei temi oggi più "delicati" in merito all'information e cyber security. Dare dei decaloghi che aiutassero chi è in difficoltà a districarsi tra eventuali dubbi o domande. Un documento che, ne eravamo certi, non sarebbe bastato, ma ponesse le fondamenta minime indispensabili.
Abbiamo voluto guardare un'azienda o una pubblica amministrazione dall'alto per vedere quali argomenti fossero da prendere in considerazione per garantire un livello di sicurezza adeguato.
Abbiamo pensato alla sicurezza infrastrutturale, a quella applicativa, alla sicurezza degli end-point, all'uso consapevole di tali strumenti da parte dei loro utilizzatori.
Abbiamo pensato che la parte infrastrutturale, per quanto ancora si possa fare per migliorare, sia tradizionalmente tra i temi sui quali c'è maggior sensibilità, sul quale è presente una maturità media più alta che su altri temi.
All'apertura dei lavori, abbiamo quindi proposto i tre temi restanti, ad un working group numeroso e molto competente. Abbiamo chiesto di dividersi in tre gruppi, per affrontare i tre pillar: applicazioni, end-user, utenti.
Dopo poco è emerso, illuminante, evidentissimo: i "tecnici", gli esperti, devono fare il loro lavoro, lo devono fare bene, lo devono fare al meglio, rispettando le leggi e le best practice di mercato. Ma anche con i migliori strumenti, gestiti al meglio, è impossibile garantire la tutela delle informazioni. È impossibile farlo senza un'utenza informata, consapevole, in grado di utilizzare gli strumenti in modo adeguato, supportata dalla tecnologia più adatta. Ma anche in grado di identificare

le truffe più comuni, in grado di percepire le "policy", le "odiose regole" non come imposizioni, ma come "guida" per districarsi in un contesto spesso ostile e pericoloso. Un gruppo popoloso, numerosissimo, di persone che troppo spesso scelgono di ignorare la sicurezza delle informazioni per comodità. Un gruppo di persone che si dovrebbe comportare "diversamente".
Per un piccolo istante si era valutato di unire il pillar "sicurezza applicativa" con il pillar "sicurezza degli end-point": parliamo in unico capitolo agli esperti, a chi può fare la differenza.
Nel solo ipotizzare questa scelta avevamo già scelto una direzione diversa. Quella a nostro parere giusta.
Si, la sicurezza applicativa è un problema importante, fondamentale, strategico, troppo spesso trascurato. Un problema per "esperti", che richiede organizzazione, competenza e strumenti. Un tema che se trascurato genera i mostri a cui ancora troppo spesso assistiamo. Bug scoperti dopo anni, bug gravissimi, incidenti gravissimi dovuti ad errori banali e noti, ciclo di vita del software inesistente, verifiche, quando svolte, inefficaci. Si, in merito alla sicurezza applicativa, è necessaria più attenzione, un approccio più metodico e serio.
Ma non basta.
Per garantire la corretta tutela dei dati è necessario fornire strumenti "adatti" … alle persone "adatte".
Così, in modo naturale e spontaneo, il gruppo che doveva lavorare sulla sicurezza degli end-point si è fuso con il gruppo che doveva lavorare sulla consapevolezza degli utenti. Più lavoravamo sul tema, più ci siamo resi conto del come non sia esclusivamente un "problema tecnologico" (se mai ci fosse stato per qualcuno il dubbio che lo fosse) o di formazione in aula.
È emerso un universo di piccoli accorgimenti da adottare, che abbiamo, ahimè, dovuto condensare e semplificare, che è passato dai più annosi problemi legati all'autenticazione, passando per l'ergonomia del software, fino ad arrivare ai metodi necessari per passare dal nozionismo al creare comportamenti virtuosi quotidiani. Ho visto svilupparsi conversazioni che ho sognato per anni. Ho sentito uno degli autori recitare "I link sono fatti per essere cliccati, gli allegati per essere aperti. Dovremmo pensare a come rendere loro evidente che quel link/allegato che stanno guardando in quel momento, morendo dalla voglia di utilizzarlo, deve essere ignorato e non pensare solo che siano ignoranti o scemi". Ho sentito parlare della frustrazione quotidiana di chi gestisce piccoli e grandi incidenti, spesso dovuti ad incuria e disattenzione. Degli utenti. Degli "esperti" che li avrebbero dovuti supportare. "Beh, se tu mi dai una app fatta così, io quel bottone li lo ignorerò per sempre!".
Lo ammetto, in alcuni momenti mi sono quasi commosso. Facile, forse, in un contesto dove molti fanno il mio lavoro, dove molti hanno la mia sensibilità. Ascoltavo, contribuivo e pensavo tra me e me "Se solo fossimo di più. Se solo la

fuori fossero tutti così. Si, abbiamo una speranza, conversazioni come questa fanno bene alla sicurezza delle informazioni. Questo piccolo documento potrebbe aiutare molti, mostrare la strada ad alcuni". Si, dedicare intere giornate di lavoro a questo progetto non è stato banale. Ma non ho avuto il benché minimo dubbio fin dall'inizio che fosse importante farlo. Ed ora, dentro il mio piccolo studio, nel cuore della notte, dopo avere riletto per l'ennesima, forse ultima, volta le pagine che state per leggere anche voi, sono più leggero, sollevato. Sento le voci degli autori che discutono tra loro. Immagino le voci di tutti quelli che saranno i loro lettori, nelle loro aziende, nei loro enti. Li sento dire ai propri colleghi "potremmo fare così" o parlare con il loro diretto superiore dicendo "vedi? Lo dico da anni! Lo dicono anche loro! Facciamo così!".
Ed immagino un futuro in cui si verificherà qualche incidente in meno, qualche data breach in meno. Immagino le informazioni che riguardano me, mia moglie, mia figlia gestiti in modo un po' più sicuro. Perché questo è tra i principali motivi per cui tutti, esperti o utilizzatori, dovremmo occuparci di information e cyber security. Per fare in modo che quello di un mondo di servizi digitali sicuri non sia solo un bel sogno. E che al nostro risveglio, ad aspettarci, non ci sia solo un cyber-incubo.

Buona lettura, quindi, ma soprattutto, buona applicazione di quanto state per leggere!

FATTORE UMANO E SICUREZZA DELL'END POINT

a cura di **Antonio Manduca** (Enea), **Carlo Bedetti** (Ministero dell'interno), **Carlo Fantini** (Ministero dell'interno), **Davide Bigoni** (Samsung), **Domenico Cuoccio** (InnovaPuglia**), Enzo Veiluva** (CSI Piemonte), **Gemma De Angelis** (Agenzia del Demanio), **Giancarlo Buzzanca** (Ministeri per i Beni e le Attività Culturali), **Gianpaolo Araco** (Senato della Repubblica), **Giovanni Mellini** (ENAV), **Giuseppe Arrabito** (Sapienza Università di Roma), **Leandro Gelasi** (Corte dei conti), **Luca Mairani** (ForcePoint), **Massimiliano Chiardoni** (Sogin), **Matteo Rigoni** (Samsung), **Paolo De Carlo** (Aizoon), **Paolo Foschi** (ForcePoint), **Pasquale Fedele** (ENEA), **Pierluigi Sartori** (Informatica Trentina), **Raffaele Visciano** (Ministero dell'Economia e delle Finanze), **Roberta Lotti** (Ministero dell'Economia e delle Finanze), **Roberto Guadagni** (ENEA), **Rosario Riccio** (Ministero dell'istruzione, dell'università e della ricerca), **Stefano Plantemoli** (Ministero dell'interno)

1. Introduzione

Key tags: obiettivi, approccio metodologico, i rischi di esposizione, importanza della messa a fattor comune

Nell'era digitale che stiamo vivendo i principi fondamentali della libertà di informazione, di espressione e di associazione, l'efficienza e la trasparenza dei servizi della Pubblica Amministrazione, la crescita e l'innovazione delle aziende si manifestano quotidianamente all'interno dello spazio Cyber. *Internet of Things*, *Big Data*, *Smart Cities*, *Social Networking*: contribuisco a far divenire lo spazio Cyber un vero e proprio campo di battaglia che ci vede impegnati nel fronteggiare l'evoluzione continua delle vulnerabilità, delle minacce e dei conseguenti attacchi. In questo contesto di estrema complessità le politiche orientate alla sicurezza informatica sono spesso mirate a privilegiare la componente tecnologica, poiché si identifica sovente il maggior pericolo come proveniente dall'esterno dell'organizzazione. In realtà la componente umana all'interno dell'organizzazione risulta spesso il vero anello debole. L'accettabilità di un rischio non dipende solo da vincoli di legge, regolamenti interni o norme tecniche ma anche da fattori non razionali connessi con la percezione dello stesso, la cultura, l'emotività, l'atteggiamento psicologico, l'esperienza del singolo.

In generale si rileva una sostanziale sottovalutazione del fattore umano, che invece deve essere considerato il primo *asset* da proteggere. Bisogna perseguire la Sicurezza come modo di essere, come stile di vita. Per queste considerazioni si ravvisa nell'accrescimento della cultura della Sicurezza, uno dei principali fattori abilitanti della trasformazione digitale, da perseguire con azioni strutturate e continue.

Per affrontare complessità e rischi del dominio Cyber, si propone nella pratica di introdurre nella propria organizzazione, prescindendo dalla sua dimensione, un modello metodologico a cui riferirsi, da potenziare nel tempo, che crei ordine nelle attività e dia il senso delle priorità. Il Modello deve prevedere una sistematica attività di identificazione, valutazione e trattamento dei rischi Cyber per il raggiungimento di un adeguato livello di sicurezza nella gestione del patrimonio informativo. Il modello deve trattare al minimo il governo dei seguenti ambiti: assett, organizzazione e processi.
Si deve, poi, operare attraverso un approccio metodologico, ricorsivo su base periodica, ispirato al ciclo di Deming[1]:

concreto in attività essenziali, suddivise in fasi di seguito descritte:

- **PLAN**: definizione degli obiettivi, del percorso di alto livello, dell'ambito, delle procedure da introdurre, dei ruoli/responsabilità (non possono mancare attività di verifica preliminare, analisi dei processi, censimento degli *asset* coinvolti, posizionamento dell'organizzazione, rilevamento gap e definizione azioni di miglioramento);
- **DO**: realizzazione degli obiettivi, erogazione di formazione e sviluppo di conoscenze (attuazione azioni di mitigazione gap/miglioramento su Organizzazione, Processi e *Asset*, accrescimento consapevolezza e cultura del patrimonio umano);
- **CHECK**: misurazione dell'adeguatezza dei processi correttivi rispetto agli obiettivi prefissati di mitigazione delle anomalie di Sicurezza rilevate in prima istanza;

[1] W. E. Deming, *Quality, Productivity and Competitivity Position*, Mit Center for Advanced Engineering Study e A. Galgano, *I sette strumenti della qualità totale*, Il Sole 24 ore Libri, Milano, 1992.

- **ACT**: recepimento dei miglioramenti identificati e attuazione delle azioni correttive e preventive. Comunicazione delle azioni e dei miglioramenti intervenuti.

La reiterazione del ciclo dipende dalla vastità e complessità dell'amministrazione/organizzazione, e andrebbe rivisitata a periodicità stabilita, almeno su base annuale. Nel modello dovranno confluire tutte le prescrizioni di conformità normative, nazionali e transnazionali, da utilizzare come leva per finalizzare gli obiettivi strategici del medesimo.

2. La sensibilizzazione come fattore abilitante alla consapevolezza del rischio cyber

Key tags: normativa, formazione, priorità, consapevolezza

Oggi l'utente è connesso al mondo attraverso il Web, i social network, le community, utilizzando l'accesso a un gran numero di contenuti e servizi.
Ognuno di questi dispositivi e/o infrastrutture IT rappresentano una "porta" di accesso potenziale per chiunque sia intenzionato a voler compromettere la nostra PA e/o azienda.
La generazione dei *Millennial* (nati tra il 1981-1996, classificazione Pew Research Center[2]) e dei *Centennials* (post-*millenial*) nasce con una smisurata confidenza all'uso della tecnologia (sono circondati da PC, internet, Tablet, *mobile*), all'utilizzo continuo dei social media e sono notoriamente "aperti" agli sviluppi e alle novità provenienti dalla rete.
Ma spesso proprio queste generazioni sono le meno attente alla sicurezza informatica, infatti attraverso la facilità di comunicazione *trust* sono più facilmente attaccabili e possono essere ingannate a compiere azioni inconsapevolmente. La velocità del mondo digitale influenza il comportamento di queste generazioni spingendole a rincorrere i tempi di attesa e risposta che vengono sempre più contratti a discapito dell'attenzione necessaria per una sicurezza Cyber.
Spesso queste generazioni non si chiedono cosa vi sia dietro un *click* o cosa comporta accettare l'utilizzo di un'*app* o verificare come opera l'*app* installata nel loro dispositivo. Spesso non riescono neanche a leggere con attenzione una *e-mail*.
Queste generazioni sono portate ad avere un rapporto fiduciario su quanto si trovi ed arrivi dalla rete e su chi fornisce i servizi desiderati. Questo comportamento cambia il modo di vedere e fruire la realtà e la mancanza di una sensibilizzazione al tema della sicurezza aumenta il ruolo del fattore umano nel rischio Cyber

[2] Defining generations: Where Millennials end and post-Millennials begin http://www.pewresearch.org/fact-tank/2018/03/01/defining-generations-where-millennials-end-and-post-millennials-begin/

In un mondo interconnesso anche un allegato *e-mail* aperto per errore da un cellulare aziendale può potenzialmente mettere in crisi l'azienda stessa.
La difesa dei sistemi informatici rappresenta quindi un elemento necessario, non prorogabile ed abilitante per lo sviluppo della nuova rivoluzione tecnologica.
Ma avere un grande sistema difensivo, delle "fortificazioni" intorno alla "cittadella" non ha senso se qualcuno in modo inconsapevole apre una porta d'accesso.
L'Italia ha intrapreso a partire dal 2013 alcune valide iniziative per rafforzare le difese Cyber: dal "*Quadro strategico nazionale per la sicurezza dello spazio cibernetico*"[3], al "*Piano nazionale per la protezione cibernetica e la sicurezza informatica*"[4]. Tuttavia, l'"insicurezza" cibernetica a livello globale - e di pari passo anche in Italia - è cresciuta in modo significativo.
Oggi il perimetro dei sistemi informativi non è più chiaramente delineato come accadeva alcuni anni fa, quando per proteggere il *data center* con i suoi preziosi dati, pochi controlli, come *firewall*, *antivirus* e controllo accessi, permettevano già di ottenere una buona protezione. Ormai non è rilevante capire se si subirà un attacco ma quando ciò accadrà e quali saranno, probabilmente, le modalità attraverso le quali poter intervenire e reagire contenendone gli impatti.
È necessario che la sicurezza si integri nei processi dell'organizzazione, proteggendone l'operatività e focalizzandosi sugli obiettivi e le criticità dell'organizzazione stessa.
Per prevenire attacchi informatici e reagire rapidamente già nelle fasi iniziali di identificazione di un attacco, al fine di contenere gli effetti negativi e soprattutto per mitigare e impedire ogni ulteriore dilagare dell'attacco ricevuto, sarebbe auspicabile:

- **dotarsi** di strumenti e processi per monitorare e gestire in modo continuo - anche attraverso l'automatizzazione - i sistemi ed i servizi, rilevando non solo gli eventi più macroscopici e "rumorosi", ma anche i segnali più deboli che possono essere indizi di *cyber attack* più subdoli e pericolosi;
- **predisporre** una centralizzazione degli aspetti di governo e controllo delle regole di sicurezza nonché una distribuzione delle operatività quotidiane di monitoraggio e di *alerting*;
- **prestare** una sempre maggior attenzione alla analisi e gestione delle vulnerabilità intrinseche dei sistemi, cercando di favorire l'adozione di soluzioni applicative "aperte", permettendo così una più facile analisi di sicurezza del codice utilizzato ed una maggior collaborazione e sinergia al livello di community.

[3] http://www.agid.gov.it/sites/default/files/leggi_decreti_direttive/quadro-strategico-nazionale-cyber_0.pdf
[4] https://www.sicurezzanazionale.gov.it/sisr.nsf/archivio-notizie/la-cyber-strategy-italiana.html

In particolare, per la PA, la grande quantità di dati a disposizione incrementa in modo proporzionale anche la necessità di garantirne la protezione ed evitarne la perdita.
Pertanto, è indispensabile:

- cambiare l'approccio per una corretta gestione del rischio Cyber, non più solo a livello di "protezione selettiva" bensì introducendo un modello organizzativo in grado di concepire una strategia di sicurezza complessiva che coinvolga non solo il sistema informativo ma tutta la Pubblica Amministrazione e le imprese interessate;
- fare sistema tra fornitori e PA prestando particolare attenzione alla crescita della consapevolezza per ogni *attore del sistema*;
- rendere consapevoli del rischio Cyber e non solo ponendo l'attenzione ai vincoli di legge, regolamenti o norme tecniche ma soprattutto ai comportamenti, fattori non razionali, alle considerazioni soggettive ed oggettive, all'immediatezza ed alla gravità delle conseguenze.

Ogni datore di lavoro della PA basandosi sulla "conoscenza del rischio Cyber" dovrebbe investire nella protezione dei propri *asset* tecnologici e dei dati/informazioni che quotidianamente gestisce. Questa attività dovrebbe essere inserita all'interno dei processi aziendali come processo progressivo per favorire la sicurezza delle informazioni e allo stesso tempo trasmettere negli *stakeholders* affidabilità e fiducia. Per questi motivi, diventa fondamentale in ogni PA la formazione del personale, dove la preparazione e l'addestramento continuo delle *persone* coinvolga tutto il personale e non solo gli specialisti IT ma innanzitutto la componente manageriale.
Il modello organizzativo, che deve tener conto della tecnologia e della *cybersecurity*, è il primo passo per sensibilizzare e coinvolgere tutti i cittadini interconnessi (in particolare i *Millennial*) ad essere più consapevoli delle loro azioni e dei rischi a cui potrebbero andare incontro.
Un cittadino capace di partecipare alla società on-line è un cittadino digitale[5]. Docenti, ricercatori e centri di ricerca di diversi Paesi nel Mondo hanno sottoscritto il "Manifesto per la Cittadinanza Digitale", dove si evidenzia come la nostra epoca sia "caratterizzata da una importante trasformazione che indica il passaggio da forme soggettive e umanistiche di interazione e cittadinanza a forme digitali, algoritmiche e info-ecologiche di partecipazione e dell'abitare"
Nell'Agenda Digitale Italiana si descrive la cittadinanza digitale come "il meta-progetto con cui la pubblica amministrazione mira a innovare il rapporto con i

[5] *Karen Mossberger, Caroline J. Tolbert e Ramona S. McNeal, Digital Citizenship: The Internet, Society, and Participation, Cambridge (United States), MIT Press Ltd, 2007, ISBN 978-02-62633-53-6*

propri cittadini, attraverso portali più usabili, Spid (identità digitale), PagoPa e altri servizi."[6]

Sono molte le iniziative avviate ma bisogna andare oltre: creare una consapevolezza chiara del rischio Cyber diventa un fattore abilitante per la crescita della cultura digitale nel nostro Paese.

In questo contesto diventa importante il ruolo delle Istituzioni che potranno fornire, in base alla trasformazione digitale, fin da subito e nel medio-lungo periodo quel supporto formativo e tecnologico per accrescere la consapevolezza del rischio Cyber e la cultura digitale nella PA. Passo indispensabile per traguardare verso una nuova definizione di Cittadino, il Cittadino Digitale Evoluto[7], che oltre ad essere fruitore di tecnologie e servizi digitali che riconosce come sicure e affidabili è consapevole delle proprie azioni e del rischio Cyber.

Il prof. Otto Scharmer, docente del Massachusetts Institute of Technology, nella sua *Theoria U* sottolinea come "*la qualità dei risultati prodotti da qualsiasi sistema dipende dalla qualità della consapevolezza dalla quale le persone nel sistema operano"*[8]. Ridurre i rischi Cyber, agendo sulla consapevolezza colloca il Cittadino Digitale Evoluto al centro del disegno della trasformazione digitale in corso nella PA.

Il Nuovo Regolamento UE 2016/679 (General Data Protection Regulation di seguito identificato come GDPR) relativo alla protezione delle persone fisiche con riguardo al trattamento e alla libera circolazione dei dati personali va in questa direzione. Infatti, il GDPR stabilisce principi e fissa obiettivi chiari ponendo il Cittadino e il suo "mondo" (i dati personali) al centro della sicurezza e dal 25 maggio 2018 è direttamente applicabile in tutti gli Stati membri.

In Italia, per armonizzare il vecchio "Codice Privacy" del 2003, il 4 settembre è stato pubblicato il D.Lgs. 101 del 10 agosto 2018[9] contenente le disposizioni per l'adeguamento della normativa nazionale vigente ai principi del GDPR.

[6] https://www.agendadigitale.eu/cittadinanza-digitale/

[7] Contenuti già anticipati da http://2018.cantieripadigitale.it/it/2018/11/26/cybersecurity-perche-fattore-umano-un-rischio/

[8] *Scharmer C. Otto,* Theory U: Leading from the Future as it Emerges, Cambridge (*United States*), *ReadHowYouWant.com Ltd, 2012, ISBN 978-1459635708*

[9] DECRETO LEGISLATIVO 30 giugno 2003, n.196 recante il "Codice in materia di protezione dei dati personali" (in S.O n. 123 alla G.U. 29 luglio 2003, n. 174) integrato con le modifiche introdotte dal DECRETO LEGISLATIVO 10 agosto 2018, n. 101, recante "Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonchè alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati)" (in G.U. 4 settembre 2018 n.205) https://www.garanteprivacy.it/documents/10160/0/Codice+in+materia+di+protezione+dei+dati+personali+%28Testo+coordinato%29

Questo deve essere uno stimolo per la PA che attraverso un approccio basato su trasparenza, sensibilizzazione e partecipazione sociale, può creare un rapporto di fiducia con il Cittadino.
Alle norme europee si aggiunge l'obbligo normativo imposto alle PA dall'Agenzia per l'Italia Digitale (AGID) che con la Circolare 2/2017 del 18 Aprile 2017 pubblica le "Misure Minime di Sicurezza ICT per le Pubbliche Amministrazioni" [10]. Una tabella esaustiva di controlli, divisi per categorie di controlli e per tipologia di livello al fine di supportare ogni PA nel contrasto alle più note e frequenti minacce informatiche.
È fondamentale sensibilizzare la persona, la società e tutelare quindi la PA in modo da coniugare la libertà individuale con la responsabilità. Innovazione digitale, trasformazione digitale, nuovi principi tecnologici, GDPR, misure minime, non si può prescindere dal creare una cultura di consapevolezza del rischio Cyber. La PA ha un compito unico ed irripetibile: l'opportunità di poter dare un impulso di cambiamento alla società, dove partendo dalla sensibilizzazione del proprio personale (a tutti i livelli) può spingere ogni Cittadino a diventare Cittadino Digitale Evoluto.
La formazione digitale a tutti i livelli avrebbe maggiore successo con il supporto della PA e in particolare iniziando dalla scuola primaria e secondaria renderebbe già la **Generazione Alpha** (le persone nate dopo il 2010) più consapevole del rischio Cyber.
Il prossimo vero obiettivo è avere una PA che sia il motore della Crescita Digitale nella società per rendere il nostro Paese più competitivo, più digitale ma anche più moderno.
In sintesi, il **governo della sicurezza Cyber** può avvenire, quindi se è presente una forte sinergia tra:

[10] CIRCOLARE 18 aprile 2017, n. 2/2017 Sostituzione della circolare n. 1/2017 del 17 marzo 2017, recante: «Misure minime di sicurezza ICT per le pubbliche amministrazioni. (Direttiva del Presidente del Consiglio dei ministri 1° agosto 2015)». http://www.gazzettaufficiale.it/eli/id/2017/05/05/17A03060/sg

In conclusione, per la PA la sfida è duplice:

- contribuire alla realizzazione del Cittadino Digitale Evoluto, favorendo la consapevolezza del rischio Cyber;
- diventare il motore della Crescita Digitale della società proponendosi propulsore di un rinnovamento atto ad accrescere la fiducia dei cittadini, la qualità e la sicurezza dei servizi erogati.

3. La determinazione delle linee guida "organizzative e comportamentali": canalizzare il modus operandi

Key tags: categorizzazione delle informazioni, comportamenti, procedure e regole

Un elemento imprescindibile per aspirare al raggiungimento di un sistema sicuro è la definizione e formalizzazione di regole comportamentali chiare e, possibilmente, semplici da applicare per gli utilizzatori. Nell'impianto documentale base dell'organizzazione deve prevedersi una metodologia per la Categorizzazione delle informazioni in modo da contenere, entro limiti accettabili, il rischio di compromissioni della riservatezza, integrità e disponibilità delle stesse. Tutte le informazioni, prodotte o ricevute, dovranno essere categorizzate ed etichettate opportunamente (anche attraverso metadati) sulla base di classi di sicurezza ad almeno tre livelli (oltre a Pubblico). Ad ogni categoria è correlato un danno potenziale e sono prescritte modalità nella trattazione come ad esempio rappresentato in tabella:

Categoria (Classe di Sicurezza)	Effetto collegato a diffusione o comunicazione a soggetti non autorizzati, interni o esterni	Prescrizioni pratiche da prevedere per gli utilizzatori
Interno	La divulgazione pur non pregiudicando la sicurezza o il business, risulta inopportuna rispetto agli interessi dell'organizzazione	No Mail personale No Social
Riservato	La divulgazione pregiudica la sicurezza o il business dell'organizzazione arrecando danni di bassa e media entità	Mail verso terzi con cifratura semplice (ZIP con psw complessa) Copia su supporto rimovibile con cifratura semplice (ZIP con psw complessa)
Segreto	La divulgazione pregiudica la sicurezza o il business dell'organizzazione arrecando danni di grave entità	Accordo di riservatezza con terze parti EndPoint cifrato Locale dove si effettua il trattamento chiuso Mail verso terzi con cifratura forte (chiavi asimmetriche) No copia su supporto rimovibile

Utilizzando quanto rilevato nelle fasi di verifica/censimento ed analisi dei processi del Modello per la Sicurezza delle Informazioni, ad ogni flusso informativo (Dato-Macrodato) insieme all' *Information Owner* coinvolto nel rilevamento, sarà associata una classe di Sicurezza che tenga conto del ciclo di vita dell'informazione, come ad esempio rappresentato in tabella:

Dato	Processo	Sottoprocesso	Macrodato	Categorizzazione
Anagrafiche paghe	HR	Amministrazione Personale	Dati personali sensibili (DPST)	Segreto
Dati su Costi interni	HR	Budget Personale	Dati contabili pre-approvazione	Segreto
			Dati contabili post approvazione	Pubblico

Reportistica	HR	Budget Personale	Reportistica operativa	Interno
Elaborati progettuali	Ingegneria	N/A	Dati di progetto	Riservato

La procedura deve prevedere regole di sicurezza nelle fasi elaborazione, duplicazione, circolazione, protezione e distruzione delle informazioni trattate.
Sulla base della mappatura dei dati gestiti all'interno dell'organizzazione e della Categoria loro associata, potranno orientarsi, con le giuste priorità, azioni pratiche di protezione degli *asset* coinvolti (tecnologici e umani), ad esempio cifratura *endpoint*, protezione dei locali, formazione specifica per gli operatori; allo stesso modo potranno opportunamente classificarsi gli *asset* coinvolti negli eventi e incidenti di sicurezza per una loro corretta gestione.

4. La condivisione delle competenze: la figura del focal point

Key tags: es. di applicazione, il ruolo del facilitatore o del master

La Direttiva del 1° agosto 2015[11] enunciava:
"*proseguire con determinazione nell'attuazione degli indirizzi strategici ed operativi identificati, ponendo in essere tutte le linee di azione necessarie sotto il profilo tecnico, organizzativo, procedurale e della collaborazione internazionale, che consentano di assicurare ai nostri cittadini uno spazio cibernetico in cui possano essere esercitate, in una cornice di sicurezza, diritti fondamentali e scambio di conoscenze, intraprese attività economiche ed intessute relazioni sociali, cogliendo così tutte le opportunità offerte dalle nuove tecnologie dell'informazione e della comunicazione*".
Partendo da queste indicazioni si sono consolidate una serie di operazioni di ampia e complessa ri-analisi della situazione sicurezza digitale presente nel nostro Paese, che hanno portato alla predisposizione di due revisioni del Piano nazionale per la protezione cibernetica e la sicurezza informatica[12] , la diffusione di un Framework nazionale di Cyber security[13], l'attuazione di misure di sicurezza per la Pubblica Amministrazione e le linee guida di sviluppo del software da parte di AgID, la decisione di centralizzazione di un CERT (Computer Emergency Response Team) unico nazionale, l'avvento di SPID, etc .

[11] https://www.sicurezzanazionale.gov.it/sisr.nsf/documentazione/normativa-di-riferimento/direttiva-1-agosto-2015.html
[12] https://www.sicurezzanazionale.gov.it/sisr.nsf/archivio-notizie/pubblicato-il-nuovo-piano-nazionale-cyber.html
[13] http://www.cybersecurityframework.it/

Per arrivare ad un risultato concreto occorre promuovere in modo massiccio tra i dipendenti e gli operatori delle Pubbliche Amministrazioni l'uso responsabile delle tecnologie. Su questo versante diventa fondamentale, soprattutto nell'ambito pubblico, l'istituzione di figure di *focal point* che operino all'interno degli uffici degli Enti. Il ruolo di queste figure è fondamentale: supportare, aiutare, diffondere tra i colleghi di ufficio la corretta sensibilità e attenzione sugli aspetti di sicurezza nell'operatività del quotidiano. Un consulto su una mail di dubbia provenienza, il suggerimento su come interpretare una prassi da seguire, un sospetto su un comportamento anomalo della propria postazione di lavoro, o il primo contatto per segnalare una emergenza di sicurezza; sono solo alcuni dei compiti che una figura di questo genere dovrebbe essere in grado di sostenere. In alcuni comuni di grandi dimensioni, dove l'organizzazione è molto complessa ed il numero di dipendenti numeroso queste figure di *utenti master* o *focal point* (che sono di riferimento non solo per gli aspetti di sicurezza, ma anche più in generale sulle componenti tecniche) è già una attuazione reale, ed i risultati ottenuto sono di molto più efficaci della semplice stesura e diffusione di Disciplinari (che comunque sono necessari anche se sono sempre in pochi a leggerli o tenerli a mente).
Con tale organizzazione è inoltre anche più semplice trasferire informazioni e aggiornamenti, concentrandoli su questi riferimenti ed ottenere più facilmente dei ritorni sul grado di incremento della sensibilizzazione. E il modello su scala minore può essere replicato anche nei comuni di medie dimensioni, creando una serie di referenti di prima linea nell'interazione con il responsabile della sicurezza.

5. Il percorso per educazione cyber: la formazione dal livello decisionale all'operativo - suggerimenti pratici

Key tags: analis dei percorsi, definizione dei target, verifica dei risultati

Una sicurezza cibernetica pensata e costruita anche in termini di competenze e cultura favorisce una giusta percezione dei rischi cyber security e rende facilmente adottabili specifici strumenti e assumibili corretti comportamenti.
Competenza e cultura si costruiscono attraverso un percorso di educazione: diventa coì fondamentale la formazione a tutti gli utenti della struttura organizzativa. In questa sezione, senza la pretesa di profondità ed esaustività, si vogliono fornire utili suggerimenti quando si decide di affrontare le questioni. Se siamo tutti più formati e consapevoli possiamo affrontare con maggiore probabilità di successo le sfide e le minacce che diventano sempre più complesse e sofisticate.
Il percorso per l'educazione all'interno dell'universo Cyber può essere composto da diversi aspetti. Di seguito proviamo a dare alcuni messaggi che forniscano una serie di osservazioni su come affrontare l'iter:

- Analizzando l'esperienza fatta finora si comprende che il fattore umano contribuisce in maniera decisa alla riuscita degli incidenti informatici, specie

quelli che sono focalizzati a catturare e ingannare la fiducia degli utenti. Poter disporre di un personale consapevole e formato rappresenta la prima linea di difesa. Una sufficiente consapevolezza e una adeguata formazione del personale deve essere l'obiettivo della componente manageriale che, in questa accezione, deve diventare lo sponsor di un percorso di educazione ossia consapevolezza e formazione.

- Il percorso di consapevolezza e formazione va progettato tenendo conto che ruoli e competenze del personale sono diversificati, il percorso di formazione va dunque personalizzato e basato sulle funzioni aziendali, sull'esposizione al rischio, sui livelli di consapevolezza e sensibilità, sulle conoscenze possedute. Il percorso deve essere di tipo continuo anche perché ci troviamo ad operare in uno scenario complesso, diversificato e mutevole.
- Prima di concentrarsi su possibili soluzioni che il mercato offre, occorre conoscere il punto di partenza ossia occorre stabilire il livello di sensibilità e consapevolezza dei rischi cyber security di ciascuno. Un *assessment* in grado di determinare le conoscenze di base individuali degli utenti, l'individuazione delle esigenze di formazione personalizzando le diverse tematiche in base alle conoscenze individuali, la possibilità di valutare l'evoluzione delle conoscenze durante il percorso educativo e alla fine dello stesso rappresenta un corretto approccio progettuale. Naturalmente in fase progettuale si può ricorrere all'aiuto di esperti in materia, avendo però idee chiaro sull'obiettivo finale. In altre parole, si tratta di costruire una roadmap che comprende i seguenti passi: *assessment* conoscenze iniziali; individuazione esigenze personalizzate per tipologia di personale; individuazione moduli formativi (modalità, aree e strumenti); avvio percorso; valutazione della corretta evoluzione; reportistica e analisi dei risultati.
- La determinazione delle conoscenze iniziali è fondamentale e può essere approcciata con più di una modalità: possono essere somministrati, ad es. questionari contenenti domande preselezionate secondo tematiche di maggiore interesse (ad es. *phishing*, protezione dei dati, navigazione Internet, …) anche ricorrendo a tecniche di "gioco"; si può ricorrere ad "attacchi simulati" magari con e-mail di *phishing* "*ready-to-use*".
- I risultati delle verifiche iniziali vanno correlati in funzione della tipologia di utente e in funzione dei comportamenti individuati: in tale modo si potrà procedere all'assegnazione di ciascun individuo ad uno o più moduli formativi. Questi ultimi, in generale, potranno riguardare le seguenti tematiche: *phishing*, protezione e distruzione dei dati, *social network*, posta elettronica, navigazione Internet, gestione credenziali, …).
- L'andamento del processo di formazione va monitorato per apportare le giuste correzioni alla sua naturale evoluzione. I risultati del processo di formazione

vanno correlai in funzione delle tematiche relative ai moduli erogati e alle tipologie di utenti. Questo fornisce due possibilità: valutare l'efficacia del processo formativo attraverso una comparazione con il livello iniziale descritto in fase di *assessment* e, in occasione di iterazione, rappresenta la nuova base di partenza.

- Spesso diventa problematico avviare un percorso di formazione e consapevolezza a 360° per tutta una serie di ragioni a partire dalla grandezza della struttura e dalle risorse economiche da dedicare, specie se si guarda al mercato puntando su eventuali soluzioni che forniscono strumenti di correlazione e reportistica automatiche. In questo caso si possono pensare a identificare i campioni di utenze in funzione di ruoli e funzioni aziendali riservandosi per i restanti un processo di sensibilizzazione alle problematiche. Un discorso a parte vale per gli amministratori di sistema o gli addetti alla sicurezza informatica: per questi il processo di formazione deve essere di natura specialistica per poter fornire loro le conoscenze adatte all'utilizzo delle nuove tecnologie e alla conoscenza delle nuove minacce.

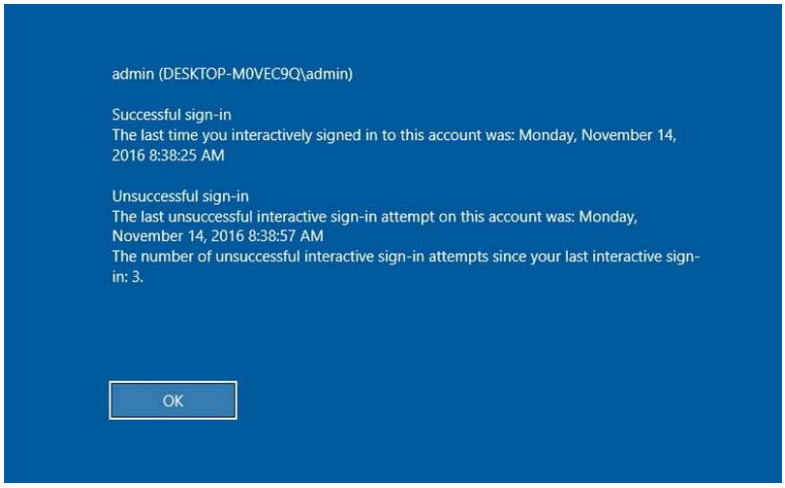
6. I punti cardine da presidiare nella difesa dell'end point

Key tags: autenticazione, protezione della mail, protezione della navigazione, accesso ai dati, cifratura delle informazioni, analisi comportamentale dei sistemi, iot, mobile, aggiornamento sistemi e backup, centralizzazione di servizi su cloud, indicatori di riscontro

6.1 Autenticazione

La definizione di *end point* come punto di accesso al sistema informatico si è andata via via ampliando per includere un sempre maggior numero di tipologie di dispositivi a partire dai "classici" laptop per finire ai tablet, agli smartphone fino ai più disparati dispositivi IoT (Internet of things), inclusi i *wearable device*.
Il problema della sicurezza degli *end point* si pone fin dall'accesso ad essi, ovvero dalla fase di autenticazione.
Inutile per una PA spendere cifre ingenti per dotarsi di sistemi di protezione *anti-virus* e *anti-ramsoware* se poi non viene correttamente gestito l'accesso degli utenti, normali e con privilegi, durante tutto il ciclo di vita delle identità.
Fondamentale è assicurarsi che l'utente che accede sia veramente chi dice di essere, attraverso sistemi di gestione delle identità e autenticazione a due fattori.
L'autenticazione a due fattori consente di irrobustire quello che è un anello debole nella catena della sicurezza di qualsiasi PA o azienda, e cioè la password degli utenti che accedono al sistema.
Oggi è meno costoso che in passato implementare un sistema di autenticazione a due fattori, basato su una OTP (*One Time Password*) che può essere comunicata

all'utente attraverso un dispositivo fisico generatore di OTP, attraverso una *app* sullo smartphone o un SMS inviato all'utente. Nonostante ciò, però, è ancora maggiormente diffusa l'autenticazione mediante password.
Per definizione nessuna password è sicura al 100% ma la sua sicurezza è inversamente proporzionale al tempo che impiegherebbe un attaccante per scoprirla; in tale situazione è fondamentale puntare sulle politiche.
Una misura che tutte le organizzazioni dovrebbero adottare a vantaggio della sicurezza degli *end point* è fornire linee guida dettagliate per la scelta di password robuste e per la conservazione di esse. Infatti, non è sufficiente implementare sistemi di controllo accessi che impongano l'utilizzo di *password* lunghe e complesse; paradossalmente si potrebbe avere un effetto contrario di indebolimento in quanto gli utenti potrebbero utilizzare sempre la stessa radice della password modificando ad ogni scadenza soltanto un progressivo numerico oppure per ricordarla potrebbero scriverla su un foglio o un database di facile accesso. Occorre che le linee guida siano ben conosciute e comprese da tutti gli utenti e occorre, altresì, mettere in atto meccanismi di verifica del rispetto delle linee guida impartite.
Una misura tecnica che si suggerisce di attivare, poiché favorisce il coinvolgimento diretto dell'utente nel controllo sull'utilizzo delle proprie credenziali, è la visualizzazione ad ogni nuovo login delle informazioni di ultimo accesso interattivo, che porta in evidenza data e ora di avvenuto ultimo accesso, ma anche dettagli sugli eventuali tentativi falliti.



Il NIST (National Institute of Standards and Technology) ha rilasciato una serie di consigli utili per la creazione di password[14]:

- Usare una passphrase, ovvero una semplice frase che richiama un'immagine nella mente ed è, quindi, facile da ricordare ma difficili da indovinare. Si può rendere la passphrase ancora più robusta sostituendo lettere con numeri o simboli, ad esempio la lettera "e" con il numero "3" o la lettera "l" con il punto esclamativo;
- Dare a ciascun account di accesso una singola passphrase.

Se si dispone di molti account/dispositivi può essere difficile ricordare tutte le password o passphrase; in tal caso può essere di aiuto un *password manager*, cioè un'applicazione progettata per conservare in modo sicuro le proprie credenziali, proprio come una "cassaforte digitale", protetta da una *master password*, necessaria per recuperare le credenziali di accesso dei vari account.

6.2 Protezione della mail

L'indirizzo di posta elettronica oggi è uno dei punti principali per i cyber-criminali per poter condurre attacchi informatici. *Phishing*, *spear phishing, malware, apt (advanced persistent threat)* sono alcune delle principali minacce per le *e-mail*. Quel che ci viene recapitato via mail può riservare le più varie sorprese: si spazia dagli allegati la cui apertura può danneggiare i nostri dati o bloccare il computer che stiamo utilizzando, per arrivare a link apparentemente innocui che se cliccati possono innescare conseguenze nefaste.
Se dovessimo immaginare un muro di cinta immaginario a nostra difesa, dobbiamo anche considerare che i proiettili moderni che abbattono il muro sono i messaggi di posta elettronica. Sono il nostro punto debole. Parliamo allora di protezione.
Proteggere la propria casella di posta significa dar luogo all'**analisi del testo che arriva via mail**, alla verifica della "eseguibilità" dei **file allegati** (qualcosa che è un programma anche se si presenta come documento inerte, magari come un PDF o un file di Word o Excel), al riscontro della presenza di virus, al *check* dei *link* che instradano verso l'installazione di **malware** e così via. Dal punto di vista strettamente legato alla fruizione dell'*e-mail*, il suggerimento è quello di applicare "fiducia zero" ai messaggi che arrivano in casella. Tutto quello che è inatteso e/o minimamente sospetto non va aperto e men che meno si deve cliccare sui *link* contenuti. Nel dubbio una telefonata al mittente può salvarci da complicazioni gravi. Questa tipologia di attacchi può essere devastante per un ente pubblico o una azienda ma anche per i dispositivi che usiamo normalmente a casa.

[14] Easy Ways to Build a Better P@$5w0rd October 04, 2017 By By: Mike Garcia https://www.nist.gov/blogs/taking-measure/easy-ways-build-better-p5w0rd

Come arginare tutto questo? Limitando la superficie di attacco, minimizzando i rischi e favorendo una buona sensibilizzazione e consapevolezza al rischio cyber. Altro suggerimento è di ridurre al minimo l'utilizzo della *e-mail* come strumento diretto di lavoro e di scambio di file. Esistono strumenti di condivisione/lavoro di gruppo molto più avanzati che permettono di lavorare in modo efficace su file condivisi garantendo uno scambio strutturato di messaggi molto più efficace dell'*e-mail*. In questo gioca un ruolo fondamentale la formazione del personale sui temi di sicurezza informatica ma soprattutto introducendo dei test di verifica ed addestramento post-formazione.
Le amministrazioni pubbliche e le aziende devono dotarsi di regolamenti e procedure interne da somministrare al personale e devono anche verificarne la correttezza e l'efficacia della loro attuazione. Occorre cominciare ad inserire dei provvedimenti disciplinari, dai più semplici ai più complessi, per quei dipendenti che, infrangendo una policy interna, creano un grave problema di sicurezza all'ente
Il percorso virtuoso per garantire la sicurezza degli account di posta elettronica passa per tre differenti approcci:

- Organizzativo
- Tecnico
- tecnologico

Di seguito saranno trattati i primi due approcci. Non verrà in questa sede approfondito il discorso tecnologico, in considerazione che oramai molti enti si appoggiano a servizi di e-mail di fornitori terzi.
L'approccio organizzativo. Ogni ente deve definire procedure e regolamenti interni per l'utilizzo degli *asset* aziendali, in particolare per gli account di posta elettronica, che devono essere sottoposti al personale e accettati senza riserve.
Gli utenti del servizio di posta elettronica hanno specifiche responsabilità di natura penale e civile ed il carico di ogni eventuale onere derivante dall'uso improprio del servizio. Inoltre, vanno impartite specifiche istruzioni per salvaguardia della riservatezza delle proprie credenziali di accesso (es. evitare di scriverle su foglietti lasciati incustoditi, di applicarle sul monitor, o di memorizzarle su file elettronici). E su questo ci vengono in aiuto ormai gli indispensabili *Password Manager*.
Per mitigare i rischi dovuti alla vulnerabilità costituita dal fattore umano (disattenzione, incompetenza, disinformazione, ecc), occorre una formazione strutturata da effettuare a tutto il personale afferente all'ente ma soprattutto occorre verificare, con test di apprendimento, il grado di apprendimento sulle seguenti tematiche:

- **riconoscere** le mail fraudolente e, in caso di dubbio, imparare ad analizzarne l' *header* (la provenienza, il mittente, i destinatari, ecc);
- **imparare** a riconoscere i *link*, potenzialmente dannosi, contenuti nella mail;

- **individuare** la tipologia di allegato che, più delle volte, è mascherato con un altro formato;
- **insegnare** alle persone di evitare di cliccare su link non affidabili presenti nelle *e-mail,*
- **non aprire** file allegati se non si è certi di cosa stiamo aprendo;
- **diffidare** di *e-mail* dubbie, che hanno lo scopo di ingannarci e di tentarci ad aprirle;
- **verificare** l'autenticità del messaggio e quella del mittente;
- **evitare** di fornire o di inserire le proprie credenziali quando ci vengono richieste per mail;
- **evitare** di inserire ed inviare *e-mail* contenenti eventuali dati di accesso ad utenze;
- **predisporre** il personale ad un'adeguata cultura di diffidenza e sospetto prima di compiere azioni sulle mail ricevute;
- **rispettare** le policy di sicurezza aziendali.

L'approccio tecnico Oltre ad effettuare la formazione è importante anche dotarsi, tra i vari regolamenti, anche di una *Password Policy* aziendale che dovrà essere approvata dal management e successivamente illustrata al personale e implementata a tutti i livelli. Una *password policy* deve poter rispettare i principi di riservatezza, integrità e disponibilità degli account e deve contenere quanto meno i seguenti principi base:

- la password è strettamente personale e non deve essere comunicata e/o condivisa con nessun'altra persona all'interno dell'organizzazione, compresi borsisti, assegnisti, collaboratori, consulenti, ecc;
- gli utenti devono prestare attenzione a fornire le proprie credenziali di accesso, a rispondere ad e-mail sospette e/o a cliccare sui link durante la navigazione web (o nella mail) al fine di contrastare possibili frodi informatiche (come il *phishing*, lo *spear phishing*, il *furto d'identità*, ecc.);
- ogni utente è responsabile di tutte le azioni e le funzioni svolte dal suo account;
- qualora vi sia la ragionevole certezza che le credenziali assegnate siano state utilizzate da terzi, l'utente dovrà cambiare immediatamente la password;
- definire criteri per la gestione di password robuste (lunghezza, tipologia di caratteri da inserire, *history password*, scadenza, cambio al primo accesso).

Inoltre, non vanno sottovalutate nemmeno le caselle di posta elettronica certificata (PEC) che possono dare adito ad un falso senso di sicurezza per il significato intrinseco della PEC stessa. Spesso le caselle di posta PEC non vengono accuratamente presidiate, non vengono inseriti requisiti di sicurezza per il rischio di non perdere eventuali mail importanti (pensiamo al protocollo informatico). Questo lo hanno compreso anche gli attaccanti, infatti sempre più spesso

assistiamo a situazioni di caselle PEC che contengono virus o che sono state oggetto di spam da parte di altre caselle PEC.
Non dimentichiamo che tutto quanto descritto sopra deve anche essere corredato dall'adeguata conformità al nuovo Regolamento Europeo sulla Protezione dei Dati (meglio noto come GDPR).

6.3 Protezione della navigazione

Oggi è impensabile poter fare a meno di Internet e dei Social sia in ambito personale, sia in ambito lavorativo. A partire da un oggetto potentissimo (*smartphone*) siamo tutti in qualche modo interconnessi, sempre e ovunque. Dalla prenotazione di un treno o di un albergo, alla verifica in tempo reale della farmacia di turno, al pagamento di una bolletta del gas e la verifica dei nostri movimenti bancari oppure nella gestione delle pratiche lavorative (es richieste provenienti da cittadini), alle banche dati relative alla normativa da applicare, al video tutorial che ci spiega come risolvere un problema lavorativo. Anche se ogni antivirus può controllare e prevenire la ricezione di virus tramite internet, sono molte le persone che vengono colpite da *malware spyware* e tentativi di *phishing*
Questo avviene non perché l'antivirus sia scadente o non faccia bene i controlli ma perché è l'utente stesso che, ingannato da falsi annunci, forza la navigazione su questi siti virus e, manualmente, scarica software o consente l'autorizzazione a codice dannoso. Come già indicato anche nelle misure di sicurezza di AgID, è oramai obbligatorio utilizzare all'interno della propria amministrazione una protezione sulla navigazione Web che implementi l'*URL Filtering* ed il *Content Filtering*
I Sistemi di *Url Filtering* partono da un elenco di siti negativi da bloccare, con la possibilità di abilitarne qualcuno se lo si ritiene utile. Il solo elenco richiede un aggiornamento continuo e non può mai essere esaustivo, perché ogni giorno nascono moltissimi nuovi siti nel mondo ed è impossibile controllarli tutti, sia manualmente che automaticamente. Per questo motivo oramai tutti i *software* attuali per la protezione della navigazione web aggiungono anche l'analisi dell'indirizzo o del contenuto.
I più efficaci sono proprio quelli che fanno analisi di contenuto (*Content Filtering*) perché decidono all'istante se i contenuti appartengono a una delle categorie che l'utente ha proibito. In questo modo funzionano anche con siti dinamici come i giornali elettronici. L'analisi del testo è intelligente perché una sola parola "negativa" non blocca un intero sito: è necessario che ci sia una combinazione di parole, con un certo peso.
Un altro sistema molto affidabile per la protezione della navigazione web riguarda l'utilizzo di soluzioni basate sulla risoluzione del nome del server a cui si vuole accedere, (DNS – *Domain Name Server*). Tali sistemi mappano continuamente gli IP

e di nomi logici di servizi Web segnalati a rischio o anomali (es domini appena creati, che poi scompaiono, etc).

6.4 La cifratura delle informazioni

La necessità di proteggere le informazioni in modo tale da evitare di essere decifrate se fossero cadute in mani sbagliate e sfruttate per acquisire un vantaggio è antica quasi quanto il mondo ed è la molla alla base della cifratura o, come suole dirsi crittografia. Il nuovo Regolamento Europeo sulla Protezione dei Dati (GDPR) ha dato nuova linfa alla problematica innalzando il livello di attenzione di pubbliche amministrazioni e imprese private sull'argomento. Nello specifico l'art. 32 del citato Regolamento afferma:

Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, il titolare del trattamento e il responsabile del trattamento mettono in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, che comprendono, tra le altre, se del caso
a) la pseudonimizzazione e la cifratura dei dati personali; (...)"[15]

Il legislatore, dunque, ha ritenuto la cifratura una efficace tecnica di protezione delle informazioni. Una organizzazione deve quindi sempre porre particolare attenzione sulla importanza e delicatezza delle informazioni trattate e eventualmente decidere di adottare tale tecnica per proteggerle. Si pensi ad es. le problematiche chi si possono innescare in presenza di un eventuale *data breach*.

Vale la pena evidenziare che la cifratura è una protezione proattiva che rende le informazioni intrinsecamente sicure diversamente da altre misure di sicurezza che hanno il compito di impedire l'accesso alle stesse. A differenza del passato, dove tutta la concentrazione era rivolta alla riservatezza delle informazioni, oggi i concetti si sono allargati a quelli che sono considerati i pilastri fondamentali della sicurezza: riservatezza, integrità e autenticità, cui si affiancano altri concetti, quali ad esempio il non ripudio. Senza entrare in tecnicismi di addetti ai lavori qui si vogliono, senza la pretesa dell'esaustività, fornire i principali concetti legati alla problematica per una visione pragmatica delle cose.

Un tipico scenario può essere così considerato: un mittente che deve inviare un messaggio ad un dato destinatario. Per fare in modo di rendere non intellegibile il suo messaggio, il mittente adotta un algoritmo di crittografia che prevede una chiave di cifratura per cifrare il messaggio in chiaro e ottenere, così, un messaggio cifrato. Il destinatario riceve il messaggio cifrato e con la chiave di decifratura ottiene il messaggio in chiaro.

[15] http://www.privacy-regulation.eu/it/32.htm

La sicurezza in questo processo sta nel mantenere sicure le chiavi che devono restare segrete.
Gli algoritmi di crittografia possono essere divisi in tre grandi famiglie, distinte tra loro sulla base delle caratteristiche tecniche che le contraddistinguono. Abbiamo:

- algoritmi simmetrici;
- algoritmi asimmetrici, o algoritmi a chiave pubblica privata;
- algoritmi di Hash, o impronta.

Nel caso di crittografia simmetrica la chiave di cifratura e la chiave di decifratura coincidono. Il mittente e il destinatario devono conoscere l'algoritmo utilizzato e la chiave è mantenuta segreta.
Nel caso di crittografia asimmetrica la chiave di cifratura e la chiave di decifratura sono diverse. Le chiavi sono generate contestualmente e il proprietario mantiene riservata una chiave (chiave privata) mentre rende conosciuta l'altra (chiave pubblica). Per ogni chiave pubblica c'è una sola chiave privata e viceversa. Cifrando con una delle due con l'altra si decifra. Cifrando con la chiave pubblica del destinatario solo quest'ultimo potrà decifrare il messaggio utilizzando la propria chiave privata, si assicura così che solo il destinatario può leggere il messaggio. Cifrando con la propria chiave privata, tutti i destinatari che decifreranno il messaggio con la corrispondente chiave pubblica si assicurano che il messaggio proviene dal proprietario della chiave privata.
Gli algoritmi di Hash hanno la caratteristica di non essere invertibili, nel senso che una volta applicati ad un testo in chiaro non è possibile ritornare a quest'ultimo partendo dal testo cifrato. Questi algoritmi producono una sequenza fissa, detta impronta del testo. Questi algoritmi hanno la funzione di garantire l'integrità dei dati e insieme agli algoritmi simmetrici e asimmetrici forniscono riservatezza, integrità e autenticità delle informazioni.
È utile avere un breve confronto tra i diversi algoritmi di cifratura poiché facilita la comprensione in termini di sicurezza.
La crittografia simmetrica può elaborare velocemente una quantità di dati elevata, le chiavi possono essere relativamente brevi, di contro deve restare segreta essendo utilizzata sia dal mittente sia dal destinatario, deve essere cambiata spesso e in presenza di numerose entità deve essere utilizzate numerose chiavi.
La crittografia asimmetrica presenta la necessità di mantenere segreta la sola chiave privata, la coppia di chiavi pubblica-privata non necessita di essere cambiata spesso. Permette di realizzate sistemi di firma digitale efficiente. La gestione delle chiavi è irrobustita e facilitata dalla presenza di una *Certification Authority* (CA), una terza parte fidata che, attraverso l'emissione di certificati digitali, garantisce l'autenticità delle chiavi pubbliche delle entità della community.
Si rimanda alla letteratura specifica gli approfondimenti tecnici.

6.5 Accesso ai dati

La protezione e la sicurezza del patrimonio di dati e informazioni gestiti è fondamentale per il corretto svolgimento della missione istituzione della struttura organizzativa e per il rispetto delle normative vigenti in tema di protezione dei dati personali a tutele delle libertà e dei diritti degli individui. L'adozione di adeguate misure a carattere organizzativo - accanto a quelle a carattere tecnico - rafforza il grado di protezione mitigando i rischi connessi con accessi non autorizzati, modifica e/o cancellazione di dati accidentali e non, comportamenti del personale, gestori e utenti in generale, incluso azioni su strumenti hardware e software. Qui si vuole catturare l'attenzione sulle componenti da tenere in considerazione allorquando si affrontano problematiche connesse all'accesso dei dati.

L'adozione di meccanismi di gestione e controllo degli accessi logici e la profilazione e autorizzazione degli utenti permette una riduzione del livello di rischio sottraendo margine alla discrezionalità ed alla libertà degli operatori.

Un sistema di controllo accessi in generale rappresenta il sistema di gestione dei dati utilizzati in un sistema informativo per autenticare gli utenti e concedere o negare i diritti di accesso a dati e risorse di sistema.

Gli utenti affluiscono a due bacini:

- Utenti interni - dipendenti, esterni che lavorano nella struttura organizzativa come consulenti,
- Utenti esterni - ossia persone non dipendenti dell'organizzazione, ma che utilizzano a vario titolo i servizi da essa erogati (es. utenti che devono accedere alle applicazioni per conto di enti in convenzione e/o obblighi normativi, cittadini).

I dati sulle identità degli utenti hanno origine da vari sistemi: HR -*Human Resources* – (per utenti interni) o altre fonti (per utenti esterni) anche attraverso appositi strumenti (console di gestione utenti). Questi dati confluiscono in quello che rappresenta il sistema di *provisioning*.

L'infrastruttura di *provisioning* alimenta il sistema di autenticazione (sistema informatico che contiene l'identità degli utenti e le relative credenziali di accesso, tipicamente "user id" e "password") e il sistema di autorizzazione (sistema informatico contenente i permessi di accesso alle applicazioni di ciascun utente).

Sono i cosiddetti amministratori di sicurezza che, mediante la console "Gestione Utenti", gestiscono le credenziali degli utenti (es. reset della password) ed attribuiscono i profili che autorizzano l'accesso a specifiche risorse applicative. Gli amministratori di sistema sono coloro che nell'ambito della struttura organizzativa si occupano della gestione operativa delle politiche di controllo accessi degli utenti (reset delle password, attribuzione dei profili che autorizzano l'accesso a specifiche risorse applicative).

Di norma la registrazione a servizi telematici esposti all'esterno in modalità self-service, mediante un'apposita applicazione di registrazione specifica del servizio telematico e, sempre in generale, non è prevista la gestione dei profili autorizzativi da parte degli amministratori, in quanto quasi sempre l'abilitazione stessa ad un servizio coincide con l'assegnazione ad uno specifico profilo.
La disponibilità di un efficiente sistema di controllo degli accessi richiede la messa in campo e l'adozione di ulteriori misure tecnico-organizzative finalizzate a:

- implementazione di criteri previsti dal modello RBAC (*Role Based Access Control*) ossia una mappatura dei profili di autorizzazione con un limitato numero di ruoli definiti nell'ambito dell'organizzazione, in modo che l'assegnazione di un singolo profilo comporti l'autorizzazione dell'utente a tutte le risorse necessarie e sufficienti a svolgere quel ruolo
- *Separation of Duties*, ossia la possibilità di imporre al sistema di controllo accessi dei vincoli di esclusione tra i profili che riguardano attività che sono incompatibili a causa della legislazione nazionale o delle norme interne ad una organizzazione,
- *Recertification*, ossia la possibilità di programmare delle revisioni periodiche dei profili assegnati ad un utente, allo scopo di verificare e confermare la sussistenza delle condizioni che hanno portato le assegnazioni dei profili agli utenti, con eventuale revoca delle stesse,
- efficace gestione del processo di autorizzazione, nel rispetto delle procedure definite, in grado di gestire correttamente, magari in maniera automatizzata, il flusso delle richieste di autorizzazione all'uso dei sistemi e delle applicazioni, dalla fase di richiesta a quella della concessione delle autorizzazioni nel sistema di Controllo Accessi,
- efficace strumento di *auditing* e *reporting*, che lavorando su dati storici, permette di disporre di tutte le informazioni in tema di:
- abilitazione degli utenti: cambi *password*, revoca/riabilitazione, inserimento/cancellazione utenti negli uffici;
- autorizzazione degli utenti: connessioni utenti/profili, (es. profilo posseduto dall'utente ad una certa data, numero di utenti possedenti un dato profilo,
- operazioni compiute da e su gli amministratori di sicurezza.

Infine, un sistema di *log management* delle registrazioni cronologiche e sequenziali delle operazioni eseguite dai programmi e dalle applicazioni, che consente di tenere sotto controllo le attività svolte, per la sicurezza dei sistemi e per il reperimento veloce di informazioni su eventuali richieste dell'autorità giudiziaria.

6.6 Il monitoraggio della rete

Il monitoraggio è un'attività essenziale per verificare che la rete stia funzionando correttamente ma viene spesso tralasciato o viene poco considerato, soprattutto in

realtà come aziende o enti locali e amministrazioni periferiche di piccole dimensioni.
Tuttavia, monitorando la rete con appositi applicativi e/o con dispositivi elettronici provvisti di software integrato (*appliance*), possiamo mettere in evidenza le molteplici criticità che un *network* può avere. Per iniziare a monitorare il nostro *network* è assolutamente necessario avere ben chiaro la topologia della rete. Diviene così importante avere una documentazione esaustiva delle connessioni dei nostri *client*, *server*, apparati *switch*, *router*, *firewall*. Questo significa recuperare il controllo. Ma questo non basta. Poiché la rete fisicamente è un insieme di cavi elettrici e di fibre ottiche connessi ad apparati *hardware*, la conoscenza di ciò che viene trasportato è basilare per poter avere un *network* "sicuro".
Per *network* sicuro, si può intendere un sistema chiuso localmente ma interconnesso, dove siano ben chiare le connessioni verso l'esterno, quindi identificare gli IXP (*Internet Exchange Point*) e le eventuali criticità che le connessioni comportano verso l'esterno.
Risulta quindi fondamentale la conoscenza di tutte le connessioni presenti nella rete, a tal proposito possono sicuramente aiutare i software IPAM (*Ip Address Management*) che, spesso in sinergia con AD (*Active Directory*) o altri sistemi di autenticazione e accreditamento alla rete, permettono puntualmente di associare indirizzi IP, nomi *Host*, indirizzi fisici (*Mac Address*). Lo step successivo è analizzare la tipologia di protocolli e di traffico che transita sull'infrastruttura.
I *software* per il monitoraggio hanno funzionalità (spesso integrate anche da *plugin* di terze parti) per misurare le performance degli apparati, delle connessioni, e le saturazioni della banda, ma soprattutto di intercettazione passiva dei dati (*sniffing*) dei pacchetti che transitano. Queste funzionalità permettono di stabilire quali apparati locali (identificati con indirizzi IP) generano eccessivi *upstream*/*downstream* ed anche la tipologia di attività in corso, desumendole da protocolli di rete e porte applicative.
L'attività sopradescritta è basilare per effettuare un "irrobustimento" (*Hardening*) delle configurazioni degli apparati informatici connessi al *network*, come *computer*, stampanti (spesso trascurate), telefonia mobile ecc..
A questo proposito, malgrado il monitoraggio della rete sia una delle *best practice* definite dalla direttiva NIS (*Network and Information Security*)[16] questa, in sostanza, non fornisce regole operative immediatamente fruibili inerenti alla *cybersecurity*.
Esiste in ogni caso una vasta gamma di validi articoli su Internet su come redigere *check-list* di irrobustimento minimizzando l'impatto di possibili attacchi informatici.
L'integrazione di software antivirus permette già di effettuare una sorta di "filtro" iniziale, evitando la propagazione di codice indesiderato, ma non sempre ciò che di malevolo transita sulla rete è costituito da virus informatici.

[16] https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive

Questi sistemi possono aiutare ad effettuare analisi puntuali ed inviare a un SIEM (combinazione di SIM *Security Information Management* e SEM *Security Event Manager*) elementi significativi, aggregandoli, per poi mettere in luce con algoritmi statistici le anomalie verificatesi.
Da ciò se ne deduce che un SIEM è uno strumento assolutamente necessario per gli amministratori di rete e per il Cybersecurity *risk* assessment, poiché innalza l'infrastruttura informatica a livelli di sicurezza ragguardevoli permettendo di gestire al meglio le vulnerabilità che immancabilmente si presentano.
Per concludere, la risposta alla domanda se esiste una rete sicura può essere soddisfatta solo a condizione di mantenere elevati livelli di aggiornamento di tutte le componenti, seguendo le indicazioni sulle CVE (*Common Vulnerabilities and Exposure*) e sulle priorità definite dai CVSS (*Common Vulnerability Scoring System*), fermo restando che bisogna sempre tener conto anche del non prevedibile e talvolta irrazionale "fattore umano".

6.7 Il controllo dispositivi mobili

Ogni politica per la sicurezza degli strumenti di mobilità dovrebbe basarsi sulla gestione centralizzata dei terminali, dei processi e dei profili utente. E' opportuno quindi non limitarsi alla gestione dei dispositivi (*Mobile Device Management* - MDM) e adottare piuttosto un sistema di gestione della mobilità aziendale (*Enterprise Mobility Management* - EMM), oltre a consentire il blocco remoto dei dispositivi e l'eliminazione da remoto dei dati nonché la configurazione rapida del nuovo terminale fornito all'utente in sostituzione del dispositivo eventualmente rubato o smarrito.
Quando si tratta di sicurezza, difatti la segmentazione riveste un'enorme importanza. Questo significa:

- **definire** i profili utente in base alle funzioni,
- **regolare** l'accesso agli strumenti per consentire la delega delle funzioni amministrative
- **stabilire** le norme per l'assegnazione dei dispositivi.

È inoltre necessario tenere conto del fatto che gli utenti possono avere a che fare con dati sensibili, che richiedono un elevato livello di protezione.
Anche la corretta identificazione delle caratteristiche del dispositivo da fornire in dotazione agli utenti interni passa attraverso una valutazione delle reali necessità, senza dimenticare che il costo del terminale è solo uno degli elementi di efficacia dell'intero progetto di mobilità.
Sia nel caso di terminali forniti dall'amministrazione o azienda che nell'eventuale caso di terminali di proprietà degli utenti (definito BYOD, ovvero *Bring Your Own Device*) è opportuno connettere alla rete informatica dell'amministrazione solo i dispositivi il cui livello di sicurezza sia stato valutato e giudicato adeguato,

analizzando ad esempio le certificazioni ottenute dal costruttore dei dispositivi nei Paesi nei quali queste norme sono consolidate.
È opportuno cifrare i dati presenti sul dispositivo, se questa funzionalità è supportata dal terminale. È altrettanto importante predisporre una tipologia di blocco dello schermo: questo semplice gesto rappresenta la prima linea di difesa contro l'accesso ai nostri dati in caso di tentativo da parte di terzi di accedere al dispositivo, ad esempio in caso di smarrimento o furto. L'impostazione base prevede l'attivazione di una password alfanumerica o di un PIN efficaci e non banali.
Ogni piano di gestione dei dispositivi mobili dovrebbe comprendere una strategia di aggiornamento del sistema operativo dei terminali: in questo senso è bene passare da una modalità di aggiornamento automatico ad una modalità che abiliti la necessaria pianificazione. In questo modo si avrà il tempo di testare e validare l'interazione tra la nuova versione del sistema operativo e le applicazioni ed i servizi già rilasciati agli utenti. È altresì consigliabile assicurare l'omogeneità tra i dispositivi a disposizione degli uffici.
La sicurezza di *app* e dati è poi il punto cardine importante quanto. È necessario prevedere un grado di controllo sugli *app store* e individuare eventuali problemi relativi alle *app* installate. In entrambi i casi, l'obiettivo è proteggere eventuali dati personali elaborati durante lo svolgimento delle attività istituzionali o aziendali.
Avvalersi di sistemi di sicurezza per creare una "lista nera" e una "lista bianca" delle *app*. Per gli utenti che gestiscono dati personali sensibili, valutare livelli di sicurezza addizionali come quelli forniti dai sistemi di segregazione dei dati.
Rispetto alle applicazioni in uso da parte degli utenti è necessario garantire che vengano aggiornate in modalità automatica, eventualmente coordinando questa fase con quella di aggiornamento del Sistema Operativo.
In generale, abilitare la memorizzazione sul dispositivo solo dei dati e delle informazioni strettamente necessarie in funzione del profilo dell'utente garantendo che gli strumenti e le *app* personali non compromettano i dati istituzionali o aziendali, poiché la responsabilità potrebbe ricadere sull'amministrazione o sull'azienda.

6.8 L'attenzione ai social

Si citano spesso tecniche di *phishing*, *spear phishing*, *pretexting*, che portano le persone ad essere il punto debole nella sicurezza Cyber. Il fattore umano è l'elemento sempre più importante. Il comportamento della persona, poco informata e sensibilizzata, diventa l'anello debole per le azioni di attacco degli *hacker* (sarebbe più opportuno definirli *cracker*), mettendo a repentaglio investimenti e piani di *risk management*. Spesso non servono tecniche di *social engineering* per avere dei problemi nella propria Istituzione/azienda. Caso emblematico è quanto accaduto nel 2015 all'emittente francese TV5Monde, dove

in un video, alle spalle di un redattore intervistato, vi erano dei fogli con le password di accesso[17]. Come dare ad un ladro le chiavi della propria porta blindata!
Anche il mondo social e le varie *app* che vi ruotano intorno (Facebook, WhatsApp, Snapchat, YouTube, ambienti social, ecc.) portano gli utenti a condividere la propria quotidianità senza essere consapevoli del rischio Cyber. Questo è dovuto ad una certa **percezione di intimità** dei social media: gli utenti non li riconoscono come minaccia, il *sentiment* di fiducia è particolarmente alto e la presenza di queste due condizioni favoriscono gli attacchi *hacker*. Il più recente rapporto annuale sulla sicurezza di Cisco[18] ha rivelato che **le truffe di Facebook sono il modo più comune per violare una rete** e, secondo un rapporto di Panda Security, **il 20% delle aziende viene infettato dal** *malware* **direttamente attraverso i social media**[19] **ed infine** l'Università di Phoenix ha reso noto che **il 66% dei cittadini statunitensi ha subito il furto di un account**[20]**.**
Le aziende e le PA devono educare i dipendenti alle policy di *Social Engineering* (ovvero l'insieme di tutte quelle **tecniche psicologiche** - non informatiche- atte a permettere il furto di informazioni) e ad usare con cautela ed intelligenza tanto il web e la posta elettronica quanto i social network.

7. Conclusioni e messaggio alle istituzioni

In conclusione, affrontare la problematica della protezione dei sistemi end point non è banale. Come tutte le circostanze che dipendono in particolare dal "fattore umano" non è semplice trovare una soluzione, un approccio generalizzato efficace. Cultura e tecnologia sono sicuramente un connubio fondamentale ma probabilmente non totalmente esaustivo. La cultura perché, per quanto comunque ci si possa sforzare per far crescere il livello di consapevolezza degli utenti resterà sempre una parte di vittime che non riesce a gestire quel irrefrenabile desiderio di click compulsivo all'apertura di ogni e-mail, che si manifesta ad esempio quando viene comunicato di aver appena vinto un cellulare di ultima generazione o viene segnalata una salatissima bolletta di un operatore telefonico, che poi riflettendo a

[17] France TV5Monde passwords seen on cyber-attack TV report https://www.bbc.com/news/world-europe-32248779
[18] Cisco 2018, Rapporto annuale sulla Cybercecurity https://www.cisco.com/c/dam/m/digital/elq-cmcglobal/witb/1661957/Final_Files_Cisco_2018_ACR_Web_IT.pdf
[19] One out of five businesses are infected by Malware through Social Media, April 5, 2016 https://www.pandasecurity.com/mediacenter/social-media/uh-oh-one-out-of-five-businesses-are-infected-by-malware-through-social-media/
[20] Cybersecurity e Social Media: tutti i rischi del 2018 secondo Sebastiano Marinaccio https://www.ninjamarketing.it/2018/01/22/cybersecurity-social-media-tutti-rischi-del-2018-secondo-sebastiano-marinaccio/

posteriori non risulta essere neanche il proprio. La gamma di esempi è vastissima ed inutile percorrerla per intero.
Dal lato dei tentatori, che hanno a disposizione una sempre più ampia quantità di risorse e di fantasia, vengono confezionate ogni giorno modalità di truffa sempre più sofisticate che portano a mettere in difficolta, e a volte a cascare nel tranello, anche gli specialisti più preparati.
Dal punto di vista della tecnologia i classici approcci basati sulle soluzioni di riconoscimento di firme (i classici antivirus e anti-malware per intenderci) da tempo da soli non sono più assolutamente sufficienti (8,4 milioni di nuovi malware identificati nel 2017), pur continuando a rimanere comunque indispensabili (senza sarebbe ancora peggio!)
È necessario introdurre altre tecnologie che possano garantire un sistema di autenticazione sicuro, un livello sempre più crescente di sicurezze della navigazione (dall'analisi del DNS, al content filtering), tecniche trasparenti di cifratura delle informazioni, soluzioni di data loss prevention adattabili al contesto, agenti dediti all'analisi continua del sistema (e delle sua "anomalie"). Ed è importante che tutto questo mix di tecnologia possa essere organizzato in modo tale da permettere di attivare quel complesso di correlazione di eventi che oggi viene definito come "analisi comportamentale dei sistemi" e cioè la capacità dei dispositivi di sicurezza di osservare il modello comportamentale degli utenti, costituendo a sua volta un modello comportamentale ed identificando i comportamenti che si discostano in modo significativo da tale modello. Questo approccio difatti potrebbe permettere non solo di individuare tempestivamente un tentativo di attacco, ma anche di sviluppare un approccio predittivo e preventivo rispetto all'insorgenza di nuove minacce.
La tecnologia deve quindi essere in grado di monitorare, acquisire ed adattarsi ai bisogni reali dell'individuo, affinché diventi sempre più mitigabile l'errore introdotto dal "fattore umano". Diventa fondamentale in ogni PA la formazione, dove la sensibilizzazione al rischio Cyber coinvolga tutto il personale non solo gli specialisti del settore IT ma innanzitutto la componente manageriale.
È indispensabile cambiare l'approccio a livello di modello organizzativo in grado di concepire una strategia di sicurezza complessiva, con particolare attenzione alla crescita della consapevolezza al rischio Cyber. Il GDPR pone il Cittadino e il suo "mondo" (i dati personali) al centro della sicurezza: la PA attraverso un approccio basato su trasparenza, sensibilizzazione e partecipazione sociale, ha l'opportunità di creare un rapporto di fiducia con i Cittadini, rendendoli più sicuri.
Per fare tutto ciò occorrono investimenti (la sicurezza non è mai gratuita, ha sempre un costo) ed in particolare nell'ambito degli uffici periferici decentrati delle pubbliche amministrazioni che ogni giorno devono lottare con difficoltà di reperimento risorse economiche, obsolescenza tecnologica, personale e gestione

del quotidiano garantendo il rispetto delle normative e dei regolamenti che non si differenziano certo per i volumi gestiti.
Occorrono investimenti in tecnologia e sviluppo delle competenze. Ma tutto ciò non può derivare solo da azioni del governo centrale; le Pubbliche Amministrazioni Locali, le Regioni e i grandi Comuni ad esempio, devono entrare in gioco pesantemente. È necessaria un'azione capillare sul territorio dove gli enti più grandi si affianchino a quelli minori per sviluppare azioni congiunte che coinvolgano i cittadini, gli uffici (centrali o periferici), le scuole, le associazioni, i media e le aziende rendendo tutti maggiormente preparati su questi temi. Un'azione che deve essere più intensa, sicuramente, di quanto oggi si sta facendo. La strada da percorrere è ancora lunga ma adesso possiamo dire che almeno dei punti di riferimento ci sono, le norme a livello nazionale ed europeo ci sono: bisogna iniziare ad applicarle seriamente, cercando di farle comprendere, cercando di farne vederne i vantaggi e le opportunità e non solo gli aspetti sanzionatori.

DECALOGO

1	Definire l'organizzazione e le regole per la sicurezza: Responsabile e controlli	Hai definito il perimetro di azione? Puoi migliorarlo
2	Definire il perimetro di azione? Si può migliorare?	Hai valutato i Rischi? Sono cambianti?
3	Valutare i Rischi e definire una soglia di accettabilità?	Hai misura il posizionamento definendo una soglia di accettabilità
4	Fornire istruzioni chiare e condivise ai dipendenti: regolamenti interni, circolari, disposizioni: aggiornare la documentazione	Hai definito una strategia di sicurezza? Puoi farla evolvere?

5	Attuare le adeguate contromisure organizzative, tecniche e tecnologiche: le Misure Minime di Sicurezza (MMS) di AgID e GDPR	Hai verificato l'applicazione dei processi base (update del sistema operativo, backup, etc)?
6	Sensibilizzare a tutti i livelli sugli aspetti di sicurezza delle informazioni	Hai sensibilizzato ed erogato la formazione a tutti i livelli? È aggiornata?
7	Effettuare formazione e addestramento del personale sui principali aspetti di sicurezza	Hai misurato la comprensione e la penetrazione di quanto applicato al punto precedente?
8	Proteggere i servizi base (mail, navigazione, sistemi, autenticazione) dell'ente.	Hai protetto i tuoi servizi base (mail, navigazione, sistemi, autenticazione, interscambio)? L'hai verificato?
9	Verificare periodicamente l'efficacia dei controlli attuati: test di addestramento del personale, verifica vulnerabilità, ecc…	Hai fornito istruzioni chiare ai dipendenti? Sono aggiornate?
10	Misurare	Hai misurato i risultati ottenuti dai punti precedenti? Se la risposta è si RIPARTIRE da 1 ☺

SICUREZZA APPLICATIVA

di **Marco Bessi** (Cast Software), **Giancarlo Cecchetti** (Umbria Digitale), **Massimo Crubellati** (Cast Software), **Domenico Cuoccio** (InnovaPuglia), **Paolo De Carlo** (Aizoon) **Marcello Di Monte** (Ministero delle Difesa), **Paolo Foschi** (Forcepoint), **Stefano Giannandrea** (Lepida), **Diego Mezzina** (Insiel), **Rosario Riccio** (MIUR), **Marco Romoli** (Cast Software), **Ettore Sala** (Laziocrea), **Michele Slocovich** (Cast Software), **Maurizio Trapanese** (AIFA), **Luca Tricca** (Arma dei Carabinieri), **Enzo Veiluva** (CSI Piemonte)

1. Introduzione

La sfida della sicurezza applicativa

Key Tags: Sicurezza delle applicazioni, Situazione attuale e trend, Principali iniziative ed azioni

La Sicurezza Informatica è un tema sempre più presente nell'agenda delle istituzioni nazionali e internazionali e, in particolare negli ultimi anni, è divenuto uno dei temi di confronto più rilevanti nel settore dell'ICT e del mercato associato a tale settore. La sicurezza informatica abbraccia l'insieme delle metodologie, tecniche, strumenti ed azioni organizzative, volte a proteggere l'ambiente informatico che include gli utenti, le reti, i sistemi, le applicazioni, i processi e i dati. L'obiettivo principale è quello di ridurre i rischi di perdita di riservatezza, integrità e disponibilità delle informazioni elaborate e/o memorizzate nei sistemi informativi, compresa la prevenzione o mitigazione degli attacchi informatici, garantendone al contempo la corretta e necessaria fruibilità.

Quando si tratta di sicurezza è poi fondamentale trattare anche gli aspetti legati alla Cultura della sicurezza, avendo chiaramente a mente come gli atteggiamenti che mettono a rischio la sicurezza sono parimenti importanti quanto la scelta di robuste soluzioni tecnologiche. Quando si tratta di sicurezza informatica si deve quindi attuare un approccio "integrato" che implica una visione a 360° su tutti i suddetti aspetti.

In generale il panorama delle minacce informatiche, ed in particolar modo quelle legate alle applicazioni, è in costante evoluzione. I fattori chiave di questa evoluzione sono legati ai rapidi progressi fatti dagli attaccanti, via via sempre più abili, al rilascio di nuove tecnologie, con inevitabile introduzione di nuove debolezze ma anche con più difese integrate, ed alla crescita della complessità dei sistemi

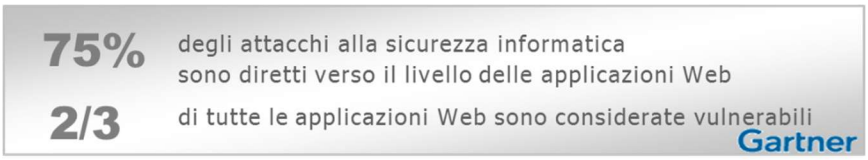
coinvolti, che ampliano continuamente il perimetro su cui occorre operare il contenimento del rischio.
Gli obiettivi degli attacchi sono spesso volti ad individuare le vulnerabilità che si celano all'interno delle applicazioni, vulnerabilità applicative che sono quasi sempre presenti all'interno del codice. La inevitabile presenza di vulnerabilità è spesso dovuta anche alle politiche adottate dalle organizzazioni in materia di qualità del software, dove l'attenzione, ed i relativi investimenti, si sono spesso concentrati prevalentemente sulla correzione delle difettosità funzionali e sull'innalzamento delle performance delle logiche applicative, sottovalutando l'applicazione di pratiche di progettazione e programmazione atte a garantire la sicurezza del codice prodotto.
L'adozione di un *Secure Software Development Life Cycle* (SSDLC) atto a considerare ed implementare idonee misure di sicurezza nel corso di tutte le fasi del ciclo di vita del software, dall'analisi alla progettazione, sviluppo, test fino alla fase di manutenzione, è divenuta oggigiorno una necessità inderogabile per rispondere alla crescente domanda di sicurezza, e per ridurre i costi indotti dal trascurare preventivamente tali aspetti.
Diverse sono le iniziative che, negli ultimi anni, si sono incentrate sulle problematiche legate alla sicurezza applicativa, promuovendo azioni di sensibilizzazione (finalizzate alle aziende e community di sviluppatori) attraverso:

- la diffusione di best practices fondamentali in materia di sicurezza applicativa (le prime tra tutte riconducibili ad una buona ingegnerizzazione del software);
- una sempre più ampia diffusione, con approfondimenti e delucidazioni, delle minacce più comuni (compresi i difetti propri dei linguaggi di programmazione);
- ed in particolar modo una considerazione delle potenziali problematiche di sicurezza fin dalle prime fasi del ciclo di sviluppo.

2. Ambienti applicativi e sicurezza

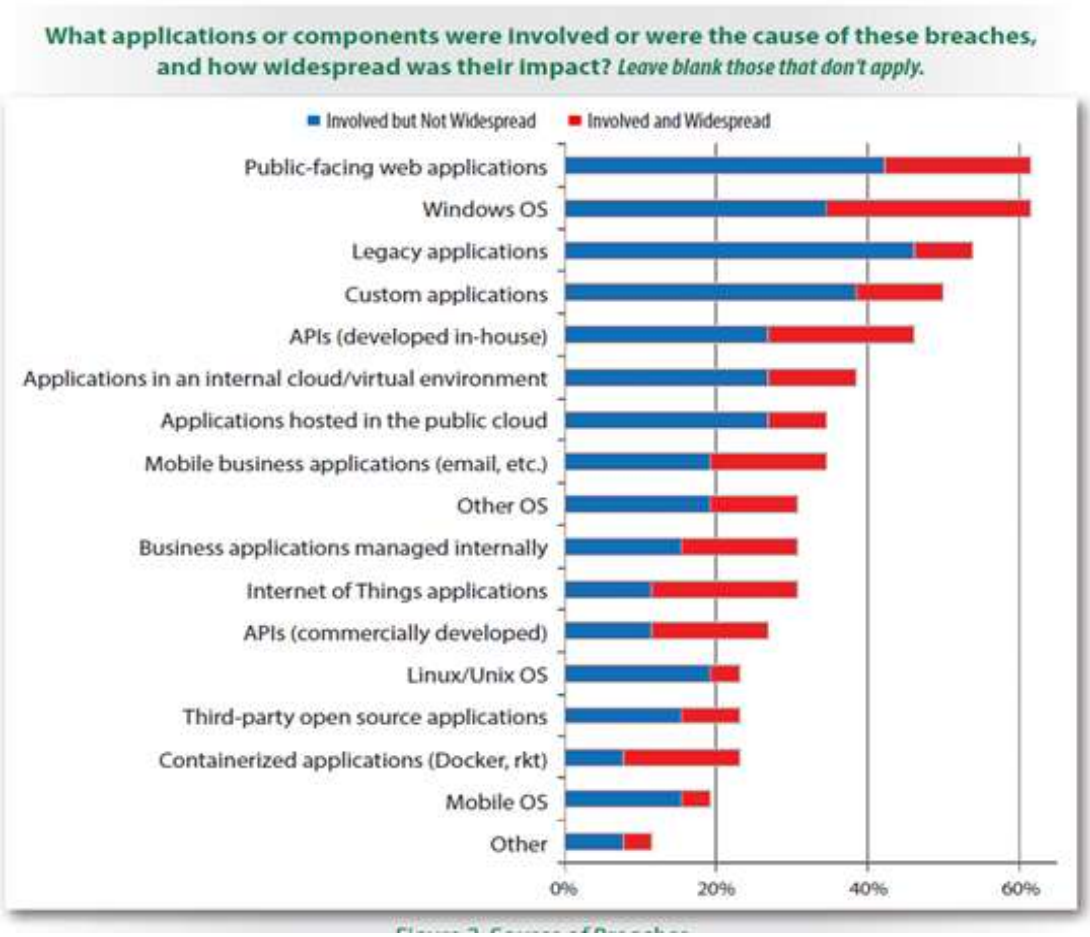
Key Tags: applicazioni web, applicazioni mobile, IoT, Cloud

Secondo Gartner, dalle analisi delle contromisure adottate per il controllo degli accessi alle infrastrutture e la messa in protezione dei dati, negli ultimi anni oltre il 75% degli attacchi sono stati indirizzati verso le applicazioni web, con conseguenti gravi danni di immagine e pesanti perdite finanziarie, e oltre la metà delle applicazioni web sono considerate vulnerabili.



Dato che la superfice di attacco si sta ampliando notevolmente rispetto al passato, in particolare man mano che il codice applicativo aumenta la presenza sul cloud, su nuovi device dell'IoT, sul Mobile e quant'altro, oggigiorno le vulnerabilità riguardano qualsiasi tipologia di ambiente.
Sempre secondo le stime di Gartner entro il 2020 però circa il 60% delle aziende digitali rischia di subire gravi perdite per incapacità di gestire il rischio digitale, ed in particolare tali incidenti saranno in relazione ai dati ed informazioni gestite da applicazioni che impiegano l'uso di dispositivi mobile o il cloud.
Secondo una analisi sui temi dell'Application Security realizzata dal SANS Institute nel 2017[21], (la ricerca comprende un ampio campione di aziende per un 72% con sede negli USA), circa un 15% delle organizzazioni ha subito negli ultimi due anni almeno un incidente direttamente collegato a problemi con le applicazioni. Dalla ricerca viene poi evidenziato che gli ambienti che hanno causato in maggior numero incidenti di scurezza sono, attualmente, nell'ordine rispettivamente: le applicazioni web esposte pubblicamente, gli ambienti Windows OS, seguiti dalle applicazioni legacy, dalle applicazioni custom e dalle API. Nella classifica la ricerca prosegue poi con gli attacchi che hanno avuto successo contro applicazioni in cloud, le App mobile e via via gli altri ambiti.

[21] https://www.sans.org/reading-room/whitepapers/application/paper/38100



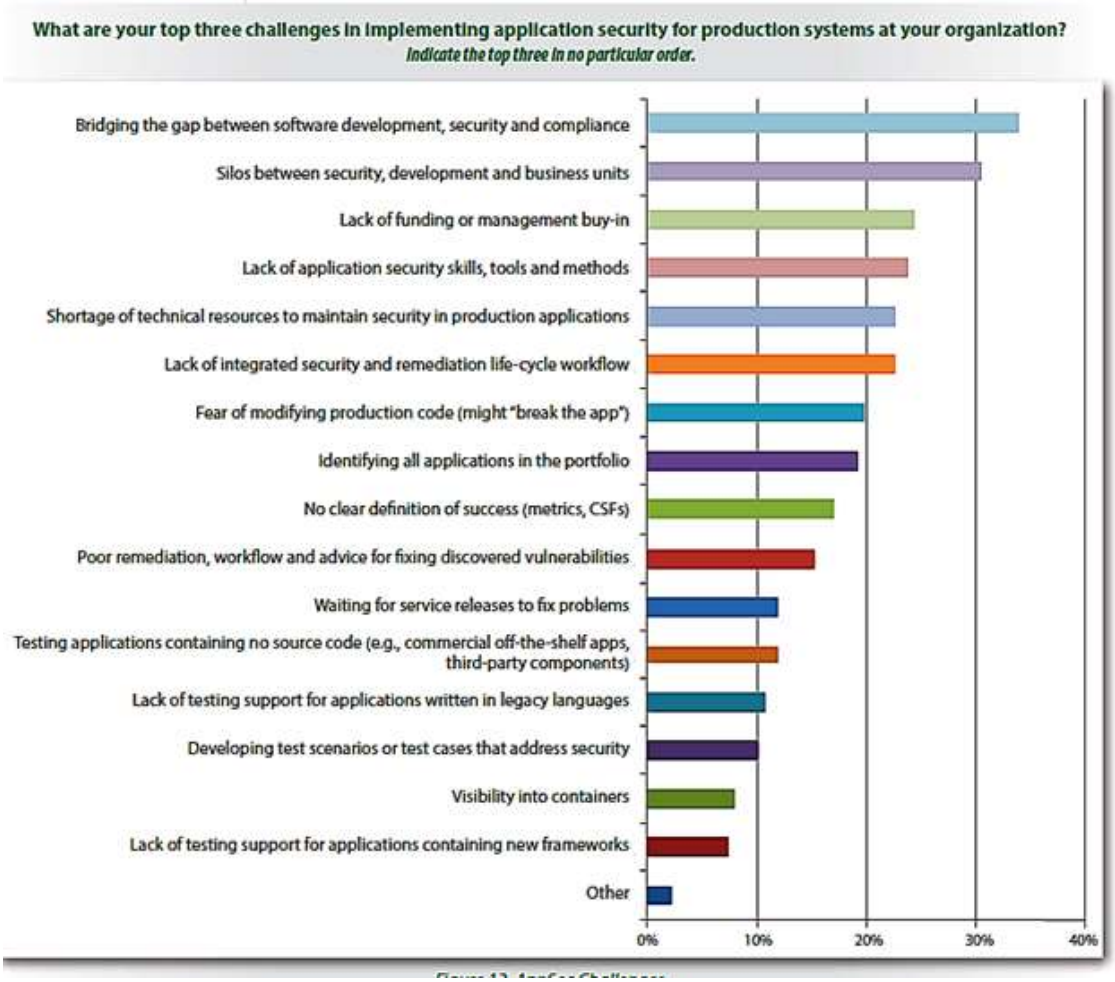
La crescita esplosiva e l'aumento della complessità di siti di eCommerce, di applicazioni mobile, e l'ampliamento e la diffusione costante delle soluzioni di Internet of Things (IoT), comportano problemi crescenti di sicurezza per via delle vulnerabilità che progetti, soluzioni, e servizi di questo tipo portano con sé. Ne sono convinti anche molti professionisti dell'IT intervistati recentemente da Forrester in tema di cybersecurity (interviste dalle quali è emerso il report "Five steps to reinforce and harden application security"[22].

In tale report si sottolinea anche la necessità di forte cooperazione tra team Security & Risk (S&R) e IT manager I&O, ribadendo il fatto che, nel contesto odierno, la diffusione dell'"Internet of everything" ha come significato indotto Internet delle 'cose hackerabili'. Nel report di Forrester, si ribadisce più volte come i S&R team non siano in grado, da soli, di coprire tutte le vulnerabilità generate dai nuovi progetti IT e dalle nuove esigenze di business digitale. Nella visione dell'analista, infatti, le persone del reparto IT, che tradizionalmente si sono sempre occupate di

[22] https://www.forrester.com/report/Five+Steps+To+Reinforce+And+Harden+Application+Security/-/E-RES127875

infrastrutture e operations sui sistemi, devono oggi supportare, attraverso meccanismi di automazione e integrazione, le pratiche di sicurezza all'interno di una '*continuous delivery pipeline*', aumentando il perimetro di azione a tutte le interazioni ed integrazioni esistenti tra apparati hardware, software, servizi web e customer data.

Valutazioni e considerazioni simili sono in parte contenute anche nei risultati della ricerca condotta nel 2017 dal SANS Institute sulla Sicurezza Applicativa citata in precedenza, da cui emerge che le organizzazioni devono rivolgere maggiore attenzione, e risorse, per superare le barriere organizzative interne, le differenze che frenano la diffusione di una cultura diffusa della sicurezza, eliminare i silos esistenti tra diversi dipartimenti (in particolar modo tra la sicurezza, lo sviluppo ed il core business dell'Organizzazione), come indicato nella tabella seguente che riporta la risposta delle Organizzazioni analizzate alla domanda su quale siano oggi le principali problematiche legate alla sicurezza applicativa.

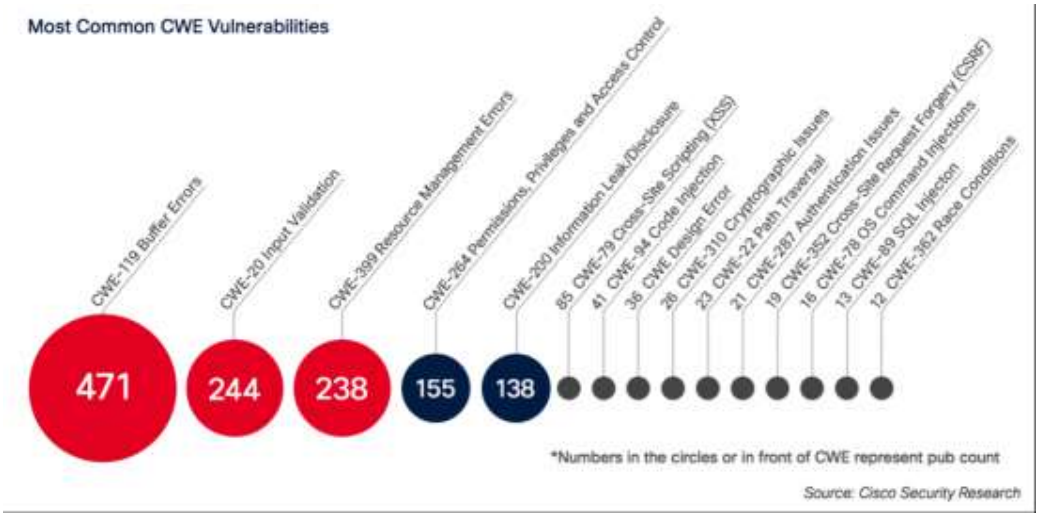


Molti degli attuali problemi di sicurezza sono derivati da errori di progettazione o di implementazione, in parte risolvibili disponendo di personale adeguatamente qualificato, ma le Organizzazioni devono investire maggiormente anche negli aspetti organizzativi connessi alla Sicurezza Applicativa oltre che nello sviluppo di adeguate competenze interne. Inoltre, per diffondere una maggiore sicurezza nel mondo dello sviluppo, serve, oltre ad una maggiore disponibilità di fondi, anche il completo supporto del management, che dovrebbe essere più coinvolto su queste specifiche problematiche.

3. La definizione del ciclo di sviluppo sicuro del software

Key Tags: SSDLC, analisi, progettazione, sviluppo, collaudo, HLD, Ciclo di vita

Gli errori di codifica del software forniscono un facile ingresso per i criminali cibernetici, che possono sfruttare le vulnerabilità del codice per compromettere i sistemi, o per veicolare attacchi e malware. Cisco, già nella sua relazione del 2015 'Midyear Security', evidenziava come alcune tipologie di errori di codifica si presentano costantemente nelle liste delle vulnerabilità più comuni (oggetto del lavoro di analisi):



Ci si chiede quindi, visto che gli stessi errori di codifica vengono di volta in volta identificati e resi noti, il perché tali errori, una volta conosciuti, non vengano opportunamente mitigati all'origine. La risposta più probabile consiste nella mancanza di sufficiente attenzione alle tematiche di sicurezza durante il ciclo di vita di sviluppo del software. In molti casi infatti, i fornitori risolvono le vulnerabilità di prodotti già presenti sul mercato, mentre sarebbe auspicabile una maggiore

attenzione e focalizzazione alle verifiche di vulnerabilità in particolare durante le fasi di sviluppo del prodotto.
Si definisce *Secure Software Development Life Cycle* (SSDLC) un ciclo di vita "sicuro" del software atto a considerare ed implementare opportune misure di sicurezza nel corso di tutte le sue fasi, in modo tale che l'azione di protezione inizi già dalla progettazione e sviluppo dell'applicativo.
Molto spesso gli aspetti di sicurezza non vengono adeguatamente considerati a partire dall'inizio del ciclo di vita del software (a volte vengono introdotti solo nelle successive fasi di test magari effettuati quando già in esercizio), e di conseguenza sono molte le vulnerabilità che vengono introdotte e/o trasmesse negli stadi successivi.
L'attuazione corretta e completa di opportune attività durante il SSDLC, conformi ai principali standard di sicurezza (OWASP, SANS, MISRA, NIST, ecc.) e, ove applicabile, ai requisiti di data protection nel trattamento del dato personale imposti dal regolamento UE n. 2016/679 (GDPR) e successive integrazioni, consente di incrementare sensibilmente il livello di sicurezza e compliance del software prodotto.
Un ciclo di sviluppo del software prevede tipicamente le seguenti fasi:

- Analisi: analizzare il contesto in cui il prodotto software deve inserirsi, le caratteristiche o requisiti che deve possedere (specifiche funzionali) ed eventualmente i costi e gli aspetti logistici relativi alla sua realizzazione (analisi di fattibilità, make or buy).
- Progettazione: definire, in funzione dei requisiti identificati, la struttura di massima (architettura di alto livello) del prodotto software e le caratteristiche dei singoli componenti (moduli).
- Implementazione: realizzare (o sviluppare) il software attraverso la programmazione (o scrittura del codice sorgente); tipicamente comprende una fase di implementazione dei singoli moduli che costituiscono il sistema, e una fase di integrazione di tali moduli a formare il sistema complessivo.
- Collaudo: verificare e validare quanto il prodotto software implementato soddisfi i requisiti individuati dall'analisi. Vengono definiti ed attuati appositi Piani di Test che includono i Test Case; in caso di mancato rispetto delle specifiche il software torna agli sviluppatori con il compito di risolvere i problemi o bug riscontrati.
- Deployment: installare e configurare il prodotto software nell'infrastruttura di esecuzione (o ambiente di produzione o esercizio) utilizzabile dagli utenti.
- Manutenzione: apportare modifiche al prodotto software successive alla messa in produzione, al fine di correggere errori attraverso patch (manutenzione correttiva), adattarlo a nuovi ambienti operativi (manutenzione adattativa) o estenderne le funzionalità (manutenzione evolutiva); la modifica al software

richiede un nuovo collaudo, sia relativo alle nuove funzionalità eventualmente introdotte, sia per accertare che le modifiche apportate non abbiano compromesso funzionalità preesistenti (collaudo di regressione).
- Documentazione: redigere la documentazione del software che deve accompagnare il software stesso sia durante le singole fasi di sviluppo sia al momento del rilascio in produzione.

Per trasformare un Ciclo di Sviluppo in un Ciclo di Sviluppo Sicuro occorre porre particolare attenzione sui seguenti aspetti:

1. Raccolta delle esigenze e definizione del perimetro di intervento:
   - raccogliere e formalizzare le informazioni sul contesto applicativo e i processi di sviluppo adottati;
   - identificare aree di miglioramento per innalzare la sicurezza del contesto applicativo e la compliance ai requisiti di sicurezza e data protection imposti dalla normativa (identificazione del perimetro di intervento);
   - identificare gli impatti organizzativi derivanti dalle azioni di cui ai punti precedenti.
2. Specifica dei requisiti di sicurezza in accordo ai requisiti tecnico-funzionali:
   - identificare le esigenze e le soluzioni di sicurezza da adottare, traducendo le esigenze stesse in requisiti di sicurezza in base alle analisi del contesto organizzativo, applicativo e tecnologico. In particolare:
   - raccolta e definizione di massima dei requisiti di sicurezza di strumenti informatici per la gestione dei processi di business sia di tipo transazionale che direzionale;
   - raccolta e definizione di massima dei requisiti di sicurezza trattati in banche dati relativi ai dati gestiti all'interno dei processi analizzati;
   - miglioramento o rinnovamento ("reengineering") dei processi analizzati e/o adozione di best practice attraverso:
   - linee guida e criteri di progettazione di applicazioni sicure (secure by design);
   - linee guida e criteri di implementazione di applicazioni sicure (secure coding);
   - linee guida e criteri di accettazione del sw, sia in caso di sviluppo interno che per i fornitori (secure testing).
3. Definizione di un High Level Design (HLD) preliminare: definizione delle alternative architetturali, modellazione delle minacce alla sicurezza e data protection e analisi delle contromisure applicabili.
4. Review del HLD, o Design refactoring, a seguito dell'applicazione delle contromisure di sicurezza individuate.
5. Implementazione e testing del sistema/applicazione/servizio sicuro attraverso:
   - programmazione sicura del codice;
   - test di sicurezza basati sull'analisi in real-time o a posteriori tramite tool di scansione del software integrati negli ambienti di sviluppo, attraverso

l'esecuzione di dinamiche, della superficie di attacco e della finestra di opportunità;
- esecuzione di test manuali sulle applicazioni in fase di esecuzione;
- individuazione e correzione delle vulnerabilità rilevate;
- attività di hardening dell'ambiente ospitante l'applicazione.

6. Manutenzione: verifiche di sicurezza periodiche; installazione e test di nuovi security improvement packages su applicazioni in esercizio.

Specifici esempi di standard e strumenti di SSDLC applicabili sono disponibili nelle "**linee guida per lo sviluppo del software sicuro"** emesse da AgID[23].

Le suddette linee guida sono suddivise nelle seguenti tematiche:

1. Linee Guida per l'adozione di un ciclo di sviluppo di software sicuro;
2. Linee Guida per lo sviluppo sicuro di codice;
3. Linee Guida per la configurazione per adeguare la sicurezza del software di base;
4. Linee Guida per la modellazione delle minacce ed individuazione delle azioni di mitigazione conformi ai principi del Secure/Privacy by Design;

Queste si inseriscono nell'ambito delle attività previste nel Piano Triennale per l'Informatica nella PA ed il relativo quadro normativo applicabile comprende:

1. Quadro Strategico Nazionale per la sicurezza dello spazio cibernetico – Presidenza del Consiglio dei Ministri – Dicembre 2013
2. PIANO NAZIONALE PER LA PROTEZIONE CIBERNETICA E LA SICUREZZA INFORMATICA Presidenza del Consiglio dei Ministri – Marzo 2017
3. Direttiva 1° agosto 2015 – Presidente del Consiglio dei ministri – Agosto 2015

Nelle linee guida, opportunamente contestualizzate per ogni Amministrazione, saranno evidenziati gli obblighi, relativi alla sicurezza, nelle fasi di design, codifica e mantenimento del software (Development Life Cycle) e la tipologia di controlli ed attività effettuati dall'Amministrazione durante l'intera fase di progetto.

Il Fornitore di software – o il team interno di sviluppo sarà quindi tenuto ad indirizzare in maniera adeguata la sicurezza del software prodotto secondo i principali standard di riferimento per lo sviluppo sicuro, adottando le best practice, risolvendo eventuali vulnerabilità ed aderendo ai termini contenuti nei contratti stipulati, garantendo il rispetto degli stessi per il personale coinvolto ed eventuali sub-contractors.

4. La definizione dei requisiti e la progettazione

Key Tags: normativa, standard, requisiti funzionali, requisiti non funzionali

La mancanza di un processo strutturato di analisi e identificazione dei requisiti di sicurezza in un progetto di sviluppo software, e di un approccio proattivo in fase di

[23] https://www.agid.gov.it/it/sicurezza/cert-pa/linee-guida-sviluppo-del-software-sicuro Cap. 8

progettazione, sono le principali cause della presenza di vulnerabilità in un software. La maggior parte di queste tipicamente derivano da comuni errori di programmazione. In base alla natura del software, dell'infrastruttura su cui opera, e della vulnerabilità, gli impatti conseguenti allo sfruttamento di una vulnerabilità da parte di un attaccante possono compromettere il software, i sistemi operativi, i database, l'ambiente condiviso o anche il sistema dell'utente/cliente, e tutte le informazioni associate.

Sull'importanza di una corretta e completa definizione dei requisiti si soffermano numerosi standard e linee guida internazionali in vari ambiti, fra i quali si possono citare:

- gestione della qualità: ISO 9000;
- gestione della sicurezza delle informazioni: ISO/IEC 27000;
- gestione del rischio: ISO 31000;
- gestione dei servizi IT: ITIL, COBIT;
- gestione dei progetti: PMBOK, Prince2, ISO 21500.

Un utile riferimento è anche la ISO/IEC 27034, una linea guida specifica per la sicurezza delle applicazioni, che prevede i seguenti cinque aspetti chiave:

- definizione dei requisiti tenendo conto degli interessi degli stakeholder, economicità e conformità;
- analisi dei rischi per l'intero ciclo di vita e per tutti i livelli di architettura;
- attuazione di opportune misure di sicurezza (es. secure coding, gestione sicura dei dati di test, ecc…);
- miglioramento continuo della sicurezza operativa tramite audit e analisi degli incidenti;
- dismissione e distruzione sicura dei dati e del software.

È fondamentale inoltre ricordare che il regolamento UE n. 2016/679 (GDPR) all'art. 25 introduce i principi di protezione dei dati fin dalla progettazione (data protection by design) e per impostazione predefinita (data protection by default), secondi i quali la protezione dei dati dovrebbe essere implementata in ogni processo industriale e tecnologico, che implichi la produzione di beni e servizi, mediante il quale vengano, ovviamente, trattati dati personali. Il titolare del trattamento dei dati personali deve adottare misure tecniche e organizzative adeguate, volte ad attuare in modo efficace i principi di protezione dei dati, al fine di garantire i diritti degli interessati. Ne deriva, quindi, che le tutte le valutazioni che il titolare del trattamento deve effettuare in tema di protezione dei dati personali devono essere compiute a monte, cioè prima di procedere al trattamento dei dati vero e proprio. Infatti, il titolare dovrà svolgere un'analisi preventiva della situazione complessiva e adottare un approccio pratico che si dovrà, a sua volta, concretizzare in una serie di attività specifiche e dimostrabili.

L'ingegneria dei requisiti (requirements engineering) consiste nel processo formale d'identificazione, analisi e validazione dei requisiti.
Ogni requisito deve essere opportunamente validato, cioè deve possedere le seguenti proprietà:

- correttezza – il requisito deve rispecchiare fedelmente il vincolo esposto dall'utente;
- completezza – i requisiti individuati devono coprire completamente i vincoli esposti dagli utenti;
- consistenza – i requisiti non devono essere incongruenti tra loro.

La gestione dei requisiti in un progetto di sviluppo software deve prevedere sia la definizione dei requisiti stessi, sia la gestione della loro evoluzione. Il processo di definizione dei requisiti non è di tipo sequenziale ma iterativo: si parte con i requisiti di business, aggiungendo poi i requisiti degli utenti, di sistema, di sottosistema software, ecc…, aumentando ad ogni iterazione il livello di dettaglio. I requisiti definiti in fase di progettazione possono subire cambiamenti durante l'esecuzione del progetto e, quindi, alcuni di essi devono poter essere modificati, aggiunti, o cancellati. Questa visione di modificabilità dei requisiti anche in corso d'opera ha di fatto aiutato le metodologie di sviluppo software Agile e DevOps a crescere ed essere adottate sempre di più a discapito del modello Waterfall.
Il modo di pensare tradizionale prevede una distinzione fra requisiti applicativi, che attengono alla logica di business del software, e quelli di sicurezza, indispensabili per garantire la capacità dell'applicazione di impedire che attacchi informatici possano causare furti di dati, inquinamento delle informazioni o arresto dell'operatività. Oggi è universalmente accettato l'uso di modelli di "security by design" e "security by default". La sicurezza cioè dev'essere considerata a partire dal design dell'applicazione e in ogni aspetto. I requisiti funzionali di sicurezza sono infatti strettamente correlati alle funzioni che verranno sviluppate e non devono essere specificati a parte, né tanto meno a posteriori. In altre parole, non si può prescindere dall'aspetto di sicurezza applicativa quando si scrivono i requisiti dell'applicazione.
I requisiti dell'applicazione possono essere di due tipi:

- requisiti funzionali: descrivono le funzionalità e i servizi offerti dal sistema e tipicamente possono essere descritti da use cases;
- requisiti non funzionali: definiscono vincoli sul sistema, ad esempio sul suo utilizzo, sulla sua manutenzione, sul suo sviluppo, ecc… Un esempio potrebbe essere un vincolo sulle performances o il fatto che, in un'interfaccia grafica, un certo elemento debba essere di colore rosso.

Anche i requisiti di sicurezza possono essere distinti in requisiti funzionali e non funzionali:

- i primi si riferiscono alle problematiche connesse con l'architettura e con le tecnologie scelte che incidono sulla logica di funzionamento dell'applicazione (ad esempio l'architettura per l'autenticazione); sono definiti e specifici per il singolo progetto;
- i secondi riguardano caratteristiche dell'ambiente operativo che incidono sulla sicurezza e più in generale possono essere ricondotti alla conformità verso specifici standard internazionalmente riconosciuti (lato software: CISQ-OMG, OWASP top 10, CWE top 25, ecc…, ma anche lato business/processo: NIS, PCI DSS, ISO/IEC 27001, ecc…); possono essere considerati cross-progetto e dovrebbero essere inseriti nella quasi totalità dei progetti.

I requisiti di sicurezza devono considerare i seguenti aspetti, identificati come CIA (o RID seguendo l'acronimo italiano):

- confidenzialità (o riservatezza): i dati possono essere acceduti solo dal legittimo proprietario o da chi, comunque, abbia le autorizzazioni necessarie. Il suo opposto è la disclosure (diffusione);
- integrità: i dati non possono essere modificati da chi non ha l'autorizzazione per farlo. Il suo opposto è l'alterazione;
- disponibilità: i dati devono essere disponibili a chi abbia le autorizzazioni necessarie nei modi e nei tempi richiesti. Il suo opposto è la distruzione.

4.1 Requisiti di sicurezza funzionali

Possono essere descritti attraverso una combinazione di casi di uso proprio e casi di uso improprio. Se i primi devono descrivere accuratamente le funzioni che l'applicazione dovrà mettere a disposizione degli utenti secondo un uso legittimo dell'applicazione, i secondi devono prevedere un'analisi dell'applicativo che si andrà a sviluppare al fine di identificare e caratterizzare i potenziali attacchi sul software. Nello stesso tempo, tali casi devono essere "sanati" dalle relative azioni di mitigazione descritte nei casi d'uso.

Ad esempio, un caso di uso improprio potrebbe essere il seguente: un utente non autorizzato tenta di accedere all'applicativo. Un potenziale rimedio potrebbe essere: tutti i tentativi di accesso all'applicativo devono essere registrati e analizzati da un sistema di Security Information & Event Management (SIEM).

Durante la fase di analisi dei requisiti deve essere definito il profilo di rischio dell'applicazione. Ciò deve avvenire attraverso la stesura di un documento che descrive gli aspetti applicativi sensibili ad attacchi malevoli e ai rischi per la sicurezza classificati in base al livello di gravità.

Tra i requisiti funzionali relativi alle problematiche di sicurezza si possono elencare:

- controllo degli accessi;
- controllo delle sessioni;
- minimizzazione della finestra di opportunità;

- minimizzazione della superficie d'attacco;
- identificazione delle minacce, adottando, ad esempio, lo schema STRIDE in cui:
  - Spoofing: l'attaccante finge di essere qualcun altro;
  - Tampering: l'attaccante altera i dati in transito o memorizzati;
  - Repudiation: l'attaccante esegue azioni che non possono essere tracciate;
  - Information disclosure: l'attaccante ottiene accesso ai dati in transito o memorizzati a cui non dovrebbe poter accedere;
  - Denial of service: l'attaccante interrompe il normale flusso operativo;
  - Elevation of privilege: l'attaccante esegue azioni non autorizzate.

4.2 Requisiti di sicurezza non funzionali

Si riferiscono all'interazione dell'applicazione nell'ambiente in cui sarà operativa (in particolare vertono su caratteristiche quali l'efficienza, l'affidabilità, la scalabilità) e alla conformità a standard e normative.
Si possono elencare fra essi:

- l'individuazione dei confini di fiducia;
- l'hardening delle componenti del sistema;
- l'interoperabilità con sistemi esterni, per esempio appartenenti ad altre organizzazioni;
- l'efficienza delle performance e dei tempi di risposta;
- la capacità di un servizio, ad esempio il numero massimo di utenti che possono collegarsi simultaneamente, il numero massimo di documenti memorizzabili, ecc…;
- i vincoli legislativi e normativi (come quelli relativi al regolamento UE n. 2016/679 (GDPR));
- la compliance agli standard internazionali di sicurezza.

In merito agli standard di sicurezza rispetto ai quali è indispensabile adeguarsi, le indicazioni riportate da OWASP offrono una guida sicura e affidabile per scrivere requisiti di sicurezza di buona qualità. L'OWASP (Open Web Application Security Project) è un'organizzazione no-profit che dal 2001 si occupa di questo specifico aspetto del software applicativo. Sebbene il focus di OWASP sia sulle applicazioni web, le stesse minacce valgono spesso per tutte le altre architetture e per tutti gli altri tipi di applicazioni. La OWASP Top Ten 2017 è la più recente classifica delle maggiori minacce per la sicurezza delle applicazioni. Una buona pratica di sicurezza richiede che il software ammesso all'esercizio non sia vulnerabile a tali minacce. Le vulnerabilità più diffuse di un'applicazione ricadono nelle seguenti categorie:

- controllo di accesso assente o scarsamente efficiente;
- mancato controllo dell'input utente o di altri servizi o applicazioni esterne;
- errato controllo delle allocazioni di memoria;
- gestione disattenta delle sessioni;
- salvataggio e trasmissione di dati in chiaro.
- Altra importante fonte di indicazioni è costituita da OMG (Object Management Group), un consorzio formato dalle aziende IT più importanti, dedicato alla formulazione di numerosi standard. In merito alla sicurezza, OMG ha prodotto l'Object Management

Group®'s cybersecurity standards, un insieme di modelli e strumenti utili per proteggere le applicazioni da accessi non autorizzati, tentativi di penetrazione fraudolenti, interruzioni del servizio, corruzione dei dati e altri problemi operativi.

4.3 Linee guida per il security by design

Senza pretesa di esaustività, di seguito viene riportato un elenco di principi di sicurezza che devono essere considerati in fase di definizione dei requisiti e di progettazione di un'applicazione software sicura:

- Modellazione delle minacce. La modellazione delle minacce consente di individuare i potenziali attacchi a cui potrebbe essere esposta una data applicazione. Richiede di scomporre l'applicazione nei suoi componenti funzionali principali, rappresentare tutte le interazioni fra questi e con l'ambiente esterno, identificare e classificare le minacce per ciascun componente, in base al rischio, al fine di sviluppare strategie di mitigazione delle minacce implementate nei progetti, nel codice e nei test case.
- Minimizzazione dei privilegi. Per la sicurezza di un'applicazione è necessario che venga predisposto un sistema di profili utenti, i quali abbiano ruoli differenti, contraddistinti dai privilegi assegnati. È importante che gli account utilizzati in fase di sviluppo non abbiano gli stessi profili utilizzati in produzione, poiché durante lo sviluppo e il collaudo, per comodità, si tende a usare privilegi troppo ampi. In produzione devono essere assegnati i privilegi di accesso e modifica agli utenti che accedono all'applicazione solo per effettuare le operazioni per le quali sono autorizzati. Si deve quindi attuare e verificare l'attuazione del principio dei "privilegi minimi".
- Separazione dei privilegi. Azioni specifiche nel software come, ad esempio, creare, eliminare o modificare determinate proprietà, devono essere consentite solo a un numero limitato di utenti con privilegi più elevati.
- Gestione delle autenticazioni e delle sessioni. L'autenticazione, o la garanzia che gli utenti siano effettivamente chi dichiarino di essere, è una sfida perenne per la sicurezza. Poiché l'autenticazione dipende in larga misura da fattori umani, è importante prevedere meccanismi come la creazione e la gestione sicura delle password, l'autenticazione a due fattori, l'utilizzo di protocolli cifrati, la scadenza delle sessioni, ecc…
- Controllo degli accessi. Ogni accesso al software da parte dell'utente deve essere controllato dal punto di vista delle autorizzazioni. Ciò consente di ridurre le possibilità di escalation dei privilegi per un utente con diritti limitati.
- Logging. È molto importante che un'applicazione tenga traccia degli avvenimenti critici che possono rappresentare un pericolo per la sicurezza. Normalmente i sistemi operativi tracciano i login degli utenti, nonché gli errori di sistema, o altri eventi. Accanto a questo log generale, ciascuna applicazione

deve produrne uno specifico configurato per le operazioni delle quali occorre tener traccia. In generale i dati da registrare comprendono i seguenti:

- login: utente, data e ora di accesso;
- logout: utente, data e ora in cui l'utente è uscito dall'applicazione;
- operazioni effettuate dall'utente: per esempio le attività sulla base dati;
- modifica dei file di configurazione di sistema;
- modifica dei dati della base dati.

Il log applicativo deve essere scritto esclusivamente dall'applicazione e nessuno, nemmeno un utente avanzato, con i privilegi di amministratore, dovrebbe esser messo in grado di modificarlo.

- Eliminazione delle vulnerabilità nel codice. Le applicazioni sono spesso soggette a vulnerabilità di tipo code injection e cross-site scripting (XSS), che consentono a un attaccante di eseguire all'interno dell'applicazione o lato client codice malevolo. Il rischio connesso alla presenza di tali vulnerabilità consiste nella potenziale violazione della sicurezza dei dati memorizzati sui server o delle informazioni presenti sui client degli utenti che utilizzano l'applicazione. I progettisti possono ridurre al minimo il rischio di attacchi di injection grazie alla comprensione di come i campi creati per l'immissione di testo possono essere utilizzati in modo improprio. Limitare la lunghezza e il tipo di testo che può essere immesso in un campo, così come sapere che alcuni caratteri devono essere rifiutati oppure ricodificati (escaping), sono misure preventive che aiutano a proteggersi da queste tipologie di attacco. Per evitare gli attacchi XSS occorre considerare quali precauzioni devono essere prese quando si esegue il rendering dell'input dell'utente nel browser. I campi liberi, come ad esempio i campi per i commenti, i forum e i campi di ricerca, insieme all'uso di Javascript e chiamate a database o ad altri servizi, devono essere oggetto di particolare attenzione.
- Gestione degli errori. Tutte le applicazioni devono gestire gli errori, producendo messaggi chiari e completi per chi è preposto alla loro manutenzione. Tuttavia, le applicazioni web devono essere configurate per mostrare all'utente non tecnico una pagina standard non contenete dettagli tecnici. Gli errori non gestiti, che finiscono col mostrare agli utenti una pagina con lo stack-trace, offrono a un eventuale malintenzionato utili informazioni sul sistema, sull'application server e sull'applicazione.
- Protezione dei dati. Devono essere identificati i dati memorizzati, trasmessi ed elaborati dall'applicazione, nonché quelli che richiedono una protezione aggiuntiva (ad esempio dati personali o particolari come definiti all'art. 9 del regolamento UE n. 2016/679 (GDPR), numeri di carte di credito, password, etc…). È una misura opportuna, ove possibile, crittografare tali dati o

memorizzarli in modo tale da proteggerne il furto, l'alterazione o l'identificabilità degli interessati dal trattamento elettronico.

- Livelli multipli di sicurezza. L'applicazione di questo principio consente di eliminare la minaccia di un "single point of security failure", ossia che il fallimento della sicurezza di una singola parte comprometta il funzionamento dell'intera applicazione.
- Sicurezza in caso di indisponibilità dell'applicazione. Anche se viene meno la disponibilità, un'applicazione deve essere comunque in grado di preservare la riservatezza e l'integrità. È necessario, pertanto, assicurarsi di progettare le impostazioni di sicurezza predefinite in modo tale che, in caso di emergenza, si neghi l'accesso e si annullino tutte le modifiche.
- Sicurezza compatibile con il facile utilizzo. La progettazione di software personalizzato deve incorporare aspetti di sicurezza in modo da non ostacolare l'user experience.

5. La sicurezza applicativa nelle gare e forniture della PA

Key Tags: Gare, forniture, capitolati

Spesso lo sviluppo di applicazioni, e in alcuni casi la progettazione o parte di essa, sono affidati da parte delle PA a fornitori esterni, pertanto risulta fondamentale sia prevedere, in modo chiaro e inequivocabile, i requisiti di sicurezza richiesti dal committente all'interno dei capitolati tecnici, sia prevedere idonei accorgimenti per assicurarsi che tutti i requisiti di sicurezza vengano effettivamente implementati.
Questo comporta la necessità di considerare, in fase di stesura dei capitolati, dei meccanismi volti ad esplicitare ed a incentivare l'effettiva implementazione dei requisiti di sicurezza richiesti.
Il pieno rispetto dei requisiti di sicurezza deve essere considerato un elemento fondamentale per il positivo collaudo della fornitura oggetto di acquisizione, ed il completo rispetto di tali requisiti deve essere esplicitamente dichiarato da parte degli operatori economici nelle relative offerte.
Inoltre, nella fase manutentiva post *Deployment*, nella manutenzione correttiva vanno considerati anche attività inerenti alla correzione di vulnerabilità di sicurezza sia per la componente sviluppata, sia per le librerie utilizzate e per gli ambienti applicativi. Possono essere utilizzate, come parametri di rifermento per tali verifiche, i bug indicati da specifiche best practices quali, ad esempio, per l'applicazione web, i controlli sulla OWASP Top 10 Most Critical Web Application Security Risks.
Da parte delle Amministrazioni va quindi tenuto conto, nella definizione dei budget e delle basi d'asta delle procedure di gara, delle attività connesse alla sicurezza applicativa (ad esempio costi connessi alle attività di verifiche di sicurezza, svolte in prima persona dall'appaltatore o affidate a terze parti), in modo tale da garantire

che gli operatori economici abbiano idonee coperture nella partecipazione alla procedura di gara per tali attività.
Occorre anche prevedere uno specifico budget per le attività interne all'Amministrazione, per la copertura delle specifiche verifiche di sicurezza, da svolgere durante le fasi di rilascio previste dalla fornitura e richieste nel capitolato e negli atti di gara.
Va ricordato che la previsione di qualsiasi requisito, e la conseguente verifica dello stesso, può avere un impatto su nuove attività da svolgere con relativi costi, che vanno quindi considerati e previsti nella definizione del budget complessivo della procedura avviata.
La "Guida tecnica all'uso di metriche per il software applicativo sviluppato per conto delle pubbliche amministrazioni" recentemente pubblicata da AgID[24] suggerisce di prevedere all'interno dei capitolati della Pubblica Amministrazione le caratteristiche non funzionali suggerite dal CISQ (Consortium IT Software Quality). Le caratteristiche non funzionali di un software che CISQ propone di misurare sono: reliability, performance efficiency, security, maintainability. Le metriche proposte da CISQ sono coerenti con le ISO 25010 e ISO 25023 (Requisiti e valutazione della qualità dei sistemi e del software). CISQ-OMG afferma che, considerata la non ambiguità di tali regole e la specifica in linguaggio formale, queste potrebbero efficacemente essere applicate nella descrizione dei requisiti non funzionali di un software da realizzare.
AgID ritiene che le regole CISQ-OMG sembrano di immediata utilità per imporre contrattualmente al fornitore vincoli di corretta programmazione, fissando soglie minime per le quattro caratteristiche previste da CISQ-OMG, che devono essere:

- superate dal software rilasciato, nei progetti di sviluppo;
- almeno mantenute dal software oggetto di interventi di manutenzione o evoluzione.

Si evidenzia come alcune recenti gare della Pubblica Amministrazione Italiana hanno richiesto servizi di security testing e quality assurance sul codice sviluppato[25], oppure la verifica delle vulnerabilità su applicazioni web-based con riferimento alla OWASP Top 10 versione 2013 e successivi aggiornamenti[26].
Si segnalano inoltre alcune gare emesse di recente dall'Unione Europea dove sono state richieste, come prerequisito di partecipazione, adeguate referenze su applicazioni software riconosciute OWASP ASVS level 3 oppure con certificazione Common Criteria EAL 2 augmented[27], mentre in altri casi sono state espressamente

[24] https://www.agid.gov.it/sites/default/files/repository_files/guida_tecnica_metriche_software.pdf
[25] Gara Enel mercato libero: Servizi di assistenza, manutenzione e sviluppo applicativo dei sistemi IT in ambito mercato libero
[26] Gara CdC-Dipe- ALCT - SAL offerta tecnica Lotto 2
[27] EU Emission Trading Scheme (ETS-DEV-2)

richieste competenze sui Processi di Accreditamento dei sistemi che trattano informazioni classificate[28]

Sempre in merito alle gare e forniture si segnala un'interessante azione, su cui hanno convenuto la quasi totalità dei CIO, CISO, e Responsabili Sicurezza e Responsabili IT sentiti sul tema nel corso dei lavori del Tavolo, consistente nel prevedere, da parte del legislatore, per tutti gli approvvigionamenti nel settore ICT uno specifico onere legato alla Sicurezza Informatica, da esplicitare appositamente in sede di gara nelle offerte presentate dai vari operatori economici, in modalità simile analoga a quanto avviene per gli oneri della sicurezza per il personale e per i lavori.

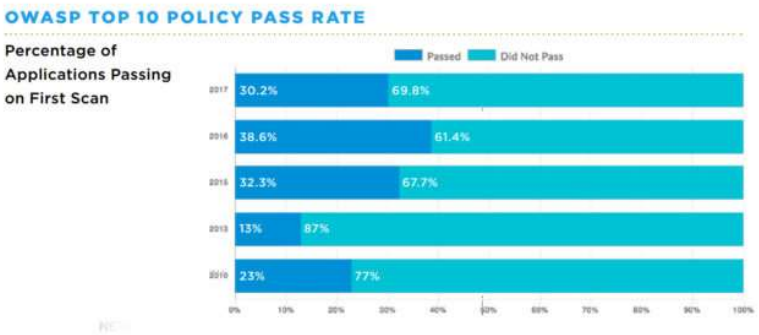
6. Le verifiche, i test e la manutenzione

Key Tags: manutenzione, vulnerabilità, test di sicurezza, SAST, DAST, PT, VA, IAST, RASP

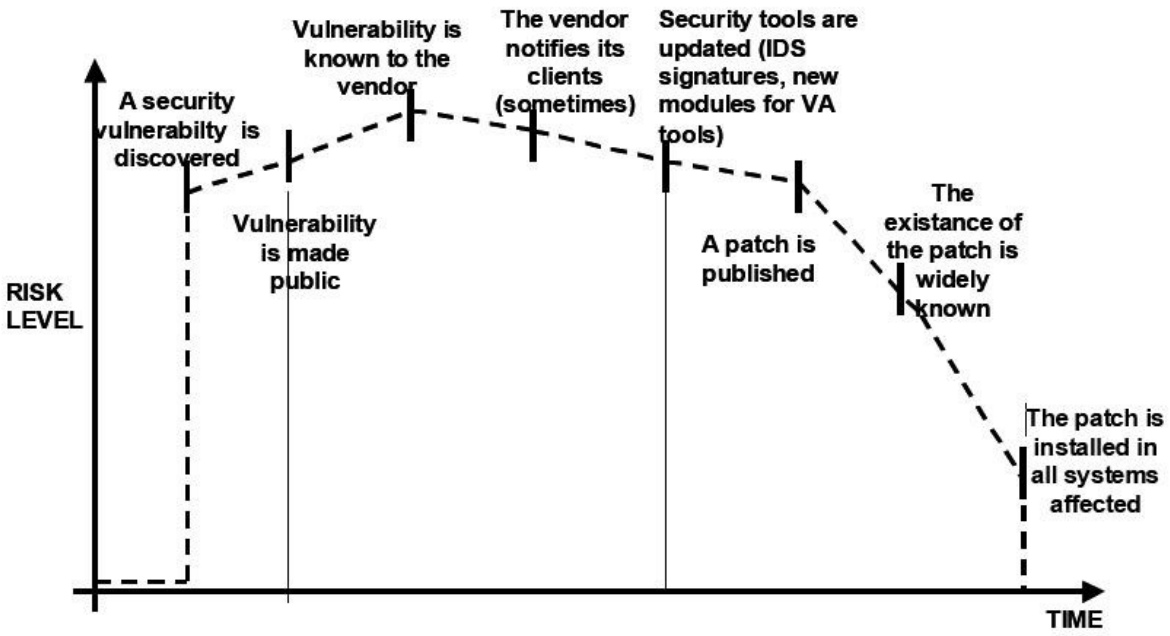
Occorre essere coscienti che il software perfetto, privo di errori/bug e che funziona senza bloccarsi, non esiste; e che gli errori presenti nel software possono mettere a rischio la sicurezza dei dati. Si può parlare di "vulnerabilità di sicurezza", anziché di "normale bug", solo quando esiste un errore/bug del software per il quale esiste altresì un metodo (exploit) per sfruttarlo a fini di attacco.

Malgrado, come anticipato in precedenza, vi sia via via una consapevolezza crescente riguardo gli aspetti di sicurezza da parte degli sviluppatori, in base a recenti verifiche condotte tra il 2016 ed il 2017 su circa 400mila scansioni di valutazione, il 70% circa delle applicazioni fallisce al primo passaggio le verifiche rispetto ai principali standard di settore per l'analisi delle vulnerabilità (rapporto Veracode 2017 SOSS - State of Software Security). In particolare (figura seguente) i test di sicurezza facevano riferimento alla percentuale di superamento del test della guida OWASP Top 10, stilata dall'organizzazione non-profit OWASP (Open Web Application Security Project).

[28] EC³IS (EEAS CORPORATE CLASSIFIED COMMUNICATION AND INFORMATION SYSTEM)



Per comprendere quali possono essere le migliori strategie di difesa è necessario conoscere il ciclo di vita che hanno le vulnerabilità di sicurezza.



Fonte OWASP

Le vulnerabilità tipicamente possono essere scoperte in uno dei seguenti modi:

- un utilizzatore di un prodotto software, casualmente, scopre un bug, non necessariamente si rende conto che il bug è una vulnerabilità, può segnalare la

cosa al produttore che analizza il caso, oppure decidere di non dar peso alla cosa;

- un potenziale attaccante, a fronte di una approfondita e con attività "professionale" di scanning, identifica un bug, identifica l'exploit utile per sfruttarla o "sviluppa" lo strumento idoneo, difficilmente informa il produttore.

Nel primo caso ci si aspetta che il produttore a fronte della segnalazione dell'utilizzatore, analizzi il caso, identifichi e codifichi la vulnerabilità, sviluppi le contromisure per poi pubblicare la relativa correzione o patch. Il rischio di sicurezza resta alto e reale per un tempo relativamente lungo, ma siamo di fronte ad un "caso" sostanzialmente sotto controllo. Se però l'utilizzatore non avvisa il produttore, il bug resta presente e latente.

Il secondo caso identifica un cosiddetto "zero-day", in cui il rischio è reale ed immediato, ma nessuno lo sa a parte il potenziale attaccante. Ovviamente questa è la situazione più pericolosa, per la quale è più difficile trovare adeguate contromisure.

Quando le vulnerabilità sono scoperte, vengono raccolte e codificate con tutte le informazioni utili (versioni del software impattate, problemi potenziali, soluzioni possibili, ecc...), quindi inserite in database di riferimento (ne esistono più di uno), assegnando ad ognuna un identificatore univoco.

Fare una verifica di vulnerabilità (o vulnerability assessment), significa sostanzialmente verificare se un'applicazione è affetta da una delle vulnerabilità presenti nelle basi dati di riferimento, che pertanto potrebbe essere sfruttata da un hacker o da un malware.

Sebbene sia possibile eseguire test di vulnerabilità, sia manualmente sia automaticamente, utilizzando appositi tools di scansione, generalmente il test comporta un effettivo livello di "sicurezza" quando eseguito in modalità semi-automatica, ovvero applicando il giusto grado di equilibrio tra attività automatiche ed azioni manuali.

In ragione della complessità delle applicazioni e dei sistemi da verificare, è infatti possibile che le verifiche e scansioni generino falsi positivi e/o falsi negativi (ovviamente più pericolosi).

Per questo motivo, la parte automatica dell'attività di Vulnerability Assessment (VA) deve essere completata mediante una fase di analisi "umana", atta a verificare se ad una vulnerabilità corrisponda o meno un metodo che ne permetta l'utilizzo (exploitation), e ad accertare che cosa l'attaccante potrebbe avere a disposizione a fronte della riuscita dell'exploit legato a tale vulnerabilità.

I VA sono quindi attività di verifica ed "effrazione" di un sistema informatico o di un'applicazione, condotti da personale "fidato" (unicamente questo li distingue, sostanzialmente, da attacchi informatici veri e propri), condotti al fine di produrre analisi e/o valutazioni delle potenziali vulnerabilità del sistema/applicazione.

Occorre comunque evidenziare che per quanto un VA sia eseguito correttamente ed "in profondità" restano comunque sempre delle analisi indicative, che non possono certificare una applicazione come sicura in assoluto (al massimo possono dire che è rispondente o meno ad un particolare standard)
Fra le tecniche utilizzabili meritano di essere ricordate:

- **static application security testing (SAST)**: utilizzo di tool che esaminano il codice binario e il codice di programmazione delle applicazioni senza mandare in esecuzione l'applicazione (ossia senza la necessità di farla girare sui sistemi nei processi di testing);
- **dynamic application security testing (DAST)**: utilizzo di strumenti che permettono di osservare in dettaglio come si comporta l'applicazione quando è in esecuzione, per scovarne imperfezioni o vulnerabilità prima che si prosegua con lo step di sviluppo successivo;
- **Interactive Application Security Testing (IAST)**: test automatizzati per l'analisi delle vulnerabilità che possono essere inseriti direttamente nell'applicazione tramite appositi sensori o agenti che analizzano continuamente tutte le interazioni delle applicazioni. Possono essere avviate manualmente, in modalità automatica o mediante una combinazione di entrambi per identificare le vulnerabilità in tempo reale. In generale non analizzano l'intero codice ma solo le componenti considerate dal test funzionale. Alcune soluzioni possono anche integrare strumenti di analisi della composizione del software (SCA) per affrontare vulnerabilità note in componenti e framework open source
- **Run-time Application Security Protection (RASP)**: una tecnologia connessa o contenuta direttamente alle applicazioni o agli ambienti runtime che sfrutta le informazioni contenute nel software in esecuzione per rilevare o bloccare gli attacchi informatici. La tecnologia RASP monitora gli input e blocca quelli che potrebbero consentire gli attacchi proteggendo al contempo l'ambiente di runtime da modifiche indesiderate e manomissioni. Quando viene rilevata una minaccia, si effettuano azioni, tra cui la chiusura della sessione di un utente, l'arresto dell'applicazione, l'avviso al personale di sicurezza e l'invio di un avviso all'utente.
- **vulnerability scanning:** utilizzo di tool utili a rendere visibili eventuali vulnerabilità a livello di sistema operativo, configurazione dei sistemi, microconfigurazioni dei web server e delle altre architetture con cui l'applicazione interagisce;
- **penetration testing (PT):** attività, prevalentemente manuali e solo parzialmente automatizzate, utili a 'validare' un precedente assessment delle vulnerabilità, perché mostrano come potrebbero avvenire gli attacchi simulando la penetrazione nei sistemi e nelle applicazioni.

Questo tipo di attività generalmente non considera l'utilizzo di tecniche potenzialmente distruttive per le applicazioni o i sistemi (che possano arrecare un qualche tipo di malfunzionamento dei sistemi coinvolti nel test) che nella realtà, attaccanti reali, potrebbe utilizzare.
I test di vulnerabilità sono in genere condotti concentrandosi su tutto ciò che potrebbe essere sfruttato per condurre attacchi, dall'interno o dall'esterno della rete in cui è in esercizio il sistema (si evidenzia che un attacco dall'interno può essere condotto sia da personale interno o da attaccanti esterni che sfruttano un sistema interno già compromesso in precedenza).
Le attività di verifica devono necessariamente essere condotte da personale specializzato, che può essere sia interno che esterno all'organizzazione. Quando vengono coinvolti dei fornitori occorre sempre stipulare un contratto che stabilisca con precisione il perimetro dei test e le responsabilità connesse all'esecuzione dell'attività, in quanto è molto sottile, dal punto di vista tecnico, la linea di demarcazione che distingue un test di vulnerabilità da un attacco informatico vero e proprio.
Purtroppo da alcune stime, diffuse nel settore, rispetto a verifiche fatte di recente su campioni significativi di Organizzazioni differenti è stato evidenziato come una gran parte di queste organizzazioni (oltre un terzo) o non esegue alcun tipo di test SAST, o non sa se viene effettuato, mentre quasi nella metà dei casi verificati non viene svolto nessun collaudo DAST; e che esiste ancora una componente notevole di Organizzazioni che continua a rilasciare codice senza prima collaudarlo rispetto alle tematiche di sicurezza.
Per iniziare da parte delle Organizzazioni un percorso di eliminazione dei difetti del software occorre che siano attivati adeguati programmi di collaudo applicativo, consistenti almeno nell'analizzare il tasso di superamento del test OWASP Top 10 (https://www.owasp.org).
Le verifiche di vulnerabilità devono accompagnare l'applicazione durante tutto il suo ciclo di vita, attraverso l'esecuzione di test diversi e appropriati allo specifico contesto. In particolare, vengono condotte nelle seguenti fasi:

- durante la fase di sviluppo software;
- prima del rilascio in produzione dell'applicazione (transition);
- durante la fase di esercizio dell'applicazione (operation).

6.1 Verifiche di sicurezza nella fase di sviluppo

Nella fase di sviluppo del software le verifiche di sicurezza devono essere condotte a partire dalla documentazione di analisi e di sviluppo, al fine di verificare completezza, coerenza, ed efficacia (teorica a questo livello) delle funzioni e dei meccanismi tecnologici implementati per la sicurezza.

A seguire, durante tutto il processo di sviluppo del prodotto software, deve essere verificata la qualità e la sicurezza del codice, sia per quanto riguarda gli algoritmi peculiari della soluzione, che per quanto attiene le integrazioni attive e/o passive, utilizzando tecniche di analisi del software statiche e/o dinamiche secondo quanto ritenuto più opportuno in relazione alle specificità del progetto.
Solo quando l'attività di sviluppo avrà portato il prodotto ad avere un adeguato grado di consistenza, sarà necessario affiancare alle precedenti verifiche, anche scansioni o penetration test eseguiti sull'applicazione in esecuzione su un ambiente di sviluppo o test, magari avviandole inizialmente in modo mirato su singole porzioni dell'albero funzionale del prodotto, per poi estenderle progressivamente al prodotto nella sua interezza.
Si precisa che quanto sopra non vale solo per i prodotti creati ex-novo, ma anche per tutti gli sviluppi successivi al primo rilascio, siano essi di manutenzione evolutiva, adattativa o correttiva.
La composizione del team di sviluppo è notoriamente un fattore critico per il livello di qualità complessiva del prodotto software che verrà rilasciato: più basso è il livello professionale degli sviluppatori, minore sarà il livello di qualità. Questo concetto si amplifica ulteriormente quando si tratta di sicurezza. In linea teorica le competenze adeguate a eseguire correttamente le verifiche di sicurezza, prevenire vulnerabilità, e produrre un'applicazione sicura, dovrebbero essere intrinsecamente presenti nel team di analisti, sviluppatori e progettisti impiegato nella realizzazione. In realtà, invece, accade spesso che durante la realizzazione, il team nel suo complesso si concentri quasi esclusivamente nella soddisfazione delle esigenze funzionali e, al limite, sull'efficienza degli algoritmi applicativi; ciò comporta, irrimediabilmente, una riduzione di attenzione alle tematiche legate alla sicurezza. È pertanto auspicabile che nei progetti di sviluppo vengano coinvolte persone che, oltre a rilevanti competenze di sviluppo software, detengano anche competenze significative sugli aspetti di sicurezza, e che vengano previste nel progetto di sviluppo specifiche milestones legate alle verifiche di sicurezza (security gates).
La mancanza di una adeguata attenzione agli aspetti di sicurezza già in fase di progettazione e sviluppo del codice, comporterà successivamente numerose e continue segnalazioni da parte degli esperti di sicurezza, a fronte delle quali l'applicazione subirà continui adattamenti, con generale discapito della qualità del prodotto realizzato. La sicurezza deve essere al centro dell'attenzione di tutto il team di progetto sin dall'inizio del ciclo di vita, ove ogni attore coinvolto (analisti, sviluppatori, progettisti) è caratterizzato ancora più, come un fattore critico nella realizzazione.

6.2 Verifiche di sicurezza nella fase di transition

Un prodotto sviluppato secondo i passi sopra descritti si presenta alla fase di transition con tutte le carte in regola per non creare sorprese né al committente né al produttore.

La fase di transition deve essere condotta, in buona sostanza, ripetendo le stesse verifiche (documentali, analisi statica e/o dinamica del software, scansioni e/o penetration test) descritte per la fase di sviluppo, con la sostanziale differenza che a condurre le verifiche non sarà più il produttore, bensì il committente, il quale ha così modo di verificare il livello di sicurezza del prodotto software che si appresta ad utilizzare dopo avere avallato il suo rilascio in esercizio.

Quando il prodotto software viene sviluppato su specifica, internamente o da un fornitore esterno, le verifiche da svolgere devono essere opportunamente definite ed inserite a livello di capitolato/contratto. Eventuali non conformità riscontrate devono quindi essere necessariamente sanate affinché il processo di transition possa completarsi. Va da sé che prodotti che fossero riscontrati come “non sicuri”, non possono essere rilasciati in esercizio, e questo deve essere espressamente previsto all’interno delle norme contrattuali.

Nel caso di sviluppo in proprio (committente e produttore coincidono quindi nello stesso soggetto), saranno i settori dell’azienda/ente deputati rispettivamente allo sviluppo, piuttosto che quelli che si occupano dell’esercizio, a dover svolgere le necessarie attività sopra descritte, rispettivamente in fase di sviluppo gli uni ed in fase di transition gli altri.

I controlli in fase di transition devono avvenire con le stesse modalità definite per tutti i rilasci successivi al primo, siano essi relativi a major o minor version dei prodotti software. Per questi rilasci, analogamente a quanto normalmente avviene dal punto di vista funzionale, è essenziale la verifica e lo svolgimento di regression test anche per quanto concerne le verifiche di sicurezza.

6.3 Verifiche di sicurezza nella fase di operation

La fase di operation inizia quindi con un prodotto testato, e valutato “sicuro”, in ambiente di produzione e che eroga correttamente i propri servizi.

È un errore quello di continuare a considerare il prodotto come “sicuro” tout court in assenza di modifiche al codice. Nuove vulnerabilità potrebbero infatti essere emerse dopo che è stato messo in produzione, o nuove tecniche di attacco potrebbero essere divenute disponibili nel frattempo. I test di vulnerabilità su prodotti in esercizio devono pertanto essere ripetuti a cadenza regolare, al fine di assicurare il mantenimento dei necessari requisiti di sicurezza, anche in assenza di modifiche o rilascio di nuove versioni.

A livello organizzativo può essere necessario disporre di specifiche aree dedicate all’esecuzione di test, ove “clonare” gli ambienti di produzione ed eseguire i test, al

fine di non avere degli impatti sulla produzione da parte dei test stessi. Una esigenza questa che può essere soddisfatta grazie alla oramai ampia diffusione di soluzioni di virtualizzazione dei sistemi.
L'esecuzione dei test di vulnerabilità su prodotti in esercizio è l'unico modo per verificare lo stato di sicurezza di applicazioni in esercizio da tempo (applicazioni legacy), per le quali non sono state eseguite le verifiche di sicurezza sopra descritte nel corso delle rispettive fasi di sviluppo e transition. Per questi prodotti in esercizio da tempo, è fondamentale, anche se non sempre scontato, avere la piena consapevolezza di ciò che viene pubblicato, in che modo ciò avviene, quali siano i servizi erogati ed i sistemi che li supportano, e quali sono le integrazioni tra essi; ovvero deve essere disponibile una piena e approfondita documentazione.
In generale una puntuale attività di assessment dello stato attuale degli applicativi è necessaria per avere coscienza dei rischi presenti nelle applicazioni in produzione, e per identificare eventuali contromisure compensative, quali ad esempio l'aggiornamento, o l'isolamento in caso di applicazioni non aggiornabili.

7. Un esempio di checkpoint organizzativo

Key Tags: Verifiche di conformità, VA, PT, Ministero della Difesa

Viene di seguito descritto il processo di acquisizione dei sistemi informativi adottato dal Ministero della Difesa, al fine di fornire un esempio di checkpoint organizzativo attuato nell'ambito della Pubblica Amministrazione.
Il processo di acquisizione di un sistema informativo all'interno del Ministero della Difesa, ha inizio con la definizione dell'esigenza operativa, intesa come documento completo anche del quadro normativo di riferimento, che rappresenta la prima formulazione scritta della necessità da soddisfare. Il citato quadro normativo dovrà essere verificato e integrato, assieme ai requisiti di sicurezza applicativa, nel Requisito Tecnico che sarà successivamente inviato alla stazione appaltante per le discendenti attività tecnico-amministrative. Tali attività si concluderanno con la stipula di un apposito Contratto Esecutivo con un Fornitore per la realizzazione/implementazione dell'applicativo secondo quanto richiesto. A completamento delle attività contrattuali, il Fornitore effettuerà la consegna del sistema sviluppato, unitamente ai documenti di seguito riportati:

- Documentazione caratteristica del sistema che comprende la descrizione delle funzionalità implementate, il manuale d'uso, i codici sorgente, ecc.;
- Certificazioni di qualità, ovvero le certificazioni di qualità in possesso del Fornitore, che sono connesse alla produzione del software;
- Dichiarazione di conformità al quadro normativo, ovvero un documento attestante l'implementazione nel software realizzato di tutte le funzionalità derivanti e previste dal complesso normativo di riferimento;

- Dichiarazione di conformità ai requisiti di sicurezza applicativa coerenti al livello di classifica richiesto.

A seguito del completamento delle attività contrattuali da parte del Fornitore, si darà corso alle attività tecnico-amministrative finalizzate alla Verifica di Conformità, prevedendo la nomina di una specifica Commissione di Collaudo che potrà richiedere, laddove necessario, una serie di controlli e verifiche di sicurezza (tabella seguente) a cura di Enti tecnici della PA dotati di specifica competenza in materia.

VERIFICA DI SICUREZZA IT

Nome campo	Valori
OWASP Web Application security test	INFORMATION GATHERING
	CONFIGURATION AND DEPLOYMENT MANAGEMENT TESTING
	IDENTITY MANAGEMENT TESTING
	AUTHENTICATION TESTING
	AUTHORIZATION TESTING
	SESSION MANAGEMENT TESTING
	INPUT VALIDATION TESTING
	ERROR HANDLING
	CRYPTOGRAPHY
	BUSINESS LOGIC TESTING
	CLIENT SIDE TESTING
Secure Coding	ANTI-BOF
	NOHCPW
Opzioni di compilazione	DEP
	ASRL
	SEH
Cifratura per i dati salvati localmente	Anonimizzazione del dato
	FIPS 140
	AES-128
	AES-192
	AES-256
	RSA 1024
	RSA 2048
	RSA 4096
Cifratura per il trasferimento dati	SSL v3

	HTTPS TLS v1.1
	HTTPS TLS v1.2
	HTTPS TLS v1.3
	Nessuna cifratura
Vulnerabilità Assessment(VA)	Not Passed (output allegato)
	Passed (output allegato)
Penetration test (PT)	Not Passed (output allegato)
	Passed (output allegato)

La Verifica di Conformità si concluderà con la redazione della Dichiarazione Tecnica di Conformità che attesta la rispondenza del software prodotto al Requisito Tecnico.
La documentazione prodotta dai processi sopra descritti costituisce la base tecnico-normativa che permetterà all'Ufficio Dirigenziale preposto (art. 17 CAD), la predisposizione della Dichiarazione di idoneità all'impiego del software realizzato. Tale dichiarazione, a firma del Capo del predetto Ufficio, costituirà la validazione e la certificazione dello stesso ai fini della distribuzione in esercizio nell'ambito della PA. Contestualmente dovrà essere definita e formalizzata una struttura di Governance dell'applicativo, attraverso la predisposizione di una specifica direttiva. In caso di variazione del quadro normativo di riferimento e/o dei requisiti di sicurezza applicativa, il processo dovrà essere ripetuto e, successivamente, sarà necessario predisporre una nuova Dichiarazione di idoneità all'impiego.
La competenza di tale processo ricadrà nell'ambito della struttura di governance predisposta.

8. Conclusioni e raccomandazioni

Il quadro tracciato nei precedenti capitoli porta a definire una situazione caratterizzata da una forte complessità nell'affrontare la sfida della sicurezza applicativa.
Considerati i dati relativi agli attacchi (per numero e tipologia) effettuati alle applicazioni negli ultimi anni, ed ai conseguenti danni indotti, l'adozione di adeguate misure di sicurezza applicativa, da introdurre in tutte le fasi del ciclo di vita del software (analisi, progettazione, sviluppo, test, e manutenzione), è diventato oggigiorno un aspetto imprescindibile per qualsiasi Organizzazione.
Adottare azioni volte a rendere sicure le applicazioni è indispensabile per salvaguardare i dati e proteggere le prestazioni dell'Organizzazione; azioni che, unite a soluzioni organizzative, a servizi di sicurezza infrastrutturali, e, in particolare, ad una cultura diffusa legata sicurezza, consentono di combattere il crimine informatico. Le organizzazioni devono poi affrontare in particolare i problemi legati

alle barriere organizzative interne, alla mancanza di una cultura diffusa della sicurezza, eliminando i silos e le distinzioni esistenti tra diversi componenti dell'organizzazione interna, con particolare riguardo ai comparti di sicurezza e di sviluppo dell'Organizzazione.

Riguardo la sicurezza applicativa le aziende devono strutturarsi e dotarsi di soluzioni adeguate a:

- migliorare la sicurezza delle applicazioni già in fase di sviluppo delle stesse, dato che lo sviluppo sicuro rappresenta una componente ormai fondamentale della strategia di business;
- testare e valutare adeguatamente il codice prima dei rilasci, con particolare riferimento alle applicazioni web e mobile, per identificarne le vulnerabilità;
- automatizzare la correlazione di risultati delle verifiche di sicurezza per applicazioni interattive, dinamiche e statiche.

Sono comunque numerose le tecniche, gli strumenti, i casi di best practices, di cui è possibile, ed auspicabile per qualsiasi Organizzazione, l'impiego per conformarsi ai principali standard di sicurezza esistenti a livello Nazionale ed Internazionale (OWASP, SANS, MISRA, NIST, ecc.).

Nel presente documento si è cercato di elencarne i principali, fornendo indicazioni e consigli metodologici, senza pretesa di esaustività, ma rimandando piuttosto agli specifici standard, tecniche, o norme in generale. Come sintesi di quanto riportato nel documento, ad ausilio del lettore, viene proposto di seguito un elenco di domande chiave che un'Organizzazione dovrebbe porsi per una corretta gestione della sicurezza delle applicazioni:

1. Nei progetti di sviluppo di nuove applicazioni, o di aggiornamento di quelle esistenti, tra i requisiti espressi (funzionali, non funzionali) sono stati compresi anche I requisiti relativi alla sicurezza?
2. Nei progetti di sviluppo di nuove applicazioni, o di aggiornamento di quelle esistenti, sono state identificate le potenziali minacce e valutati i rischi correlati al fine di definire adeguate contromisure?
3. Nei progetti relativi alle nuove applicazioni o all'aggiornamento di quelle esistenti viene previsto un'apposita componente di budget per la sicurezza (es. per attività di testing)?
4. Nei progetti di sviluppo software sono adottate best practice per lo sviluppo sicuro (SSDLC – Secure Software Development Lifecycle)?
5. Sono definiti e previsti dalle procedure interne all'organizzazione adeguati momenti di verifica della sicurezza, o checkpoint organizzativi coerenti con la natura dell'Organizzazione, durante tutte le fasi del ciclo di vita delle applicazioni (sia in fase di sviluppo, sia in fase di transition sia durante l'esercizio) e per presidiare l'adozione delle contromisure identificate?

6. Negli affidamenti per lo sviluppo di applicazioni sono previsti nei capitolati e documentazione di gara i requisiti di sicurezza, ed è previsto che questi requisiti siano verificati in fase di collaudo di accettazione del prodotto?
7. Viene eseguito periodicamente un censimento delle applicazioni in esercizio (e delle applicazioni legacy), dei sistemi che le ospitano, e svolte adeguate verifiche di sicurezza sulle applicazioni e sui sistemi?
8. Vengono utilizzate le informazioni di ritorno dalle verifiche di sicurezza, dai log delle applicazioni e dagli incidenti di sicurezza per definire adeguate contromisure atte a contrastare le vulnerabilità riscontrate e migliorare in modo continuativo il livello di sicurezza dei sistemi e delle applicazioni?
9. Il personale tecnico, e l'intera organizzazione, dispone di adeguate competenze relative alla sicurezza delle applicazioni ed effettua continui aggiornamenti sui trend e sui rischi connessi alla sicurezza applicativa per rimanere aggiornati sulle nuove minacce e vulnerabilità e per applicare tempestivamente gli aggiornamenti di sicurezza disponibili ai sistemi e alle applicazioni in esercizio?
10. Esistono o sono previsti specifici ambienti di test per consentire la gestione della sicurezza anche durante l'esercizio dell'applicazione, senza impattare sul servizio?

I PROTAGONISTI DEL CANTIERE

Alessio Pennasilico
Information & Cyber Security Advisor - Membro Comitato Direttivo Clusit

Davide Bigoni
Project Manager, Samsung Electronics Italia

Gianpaolo Araco
Capo Ufficio Strategie dell'Informatica, Servizio informatica, Senato della Repubblica

Antonio Bosio
Product & Solutions Director, Samsung Electronics Italia

Giuseppe Arrabito
Responsabile della sicurezza delle informazioni per il Centro InfoSapienza, Sapienza Università di Roma

Giancarlo Buzzanca
Responsabile Area sviluppo applicazioni web/informatiche, sicurezza informatica, Ministero per i beni e le attività culturali

Carlo Bedetti
Responsabile reti e cybersecurity del CED, Direzione centrale dei servizi elettorali, Ministero dell'Interno

Giancarlo Cecchetti
Responsabile Area Sistemi e Reti, Umbria Digitale

Marco Bessi
Solution Design Manager, Cast

Massimiliano Chiardoni,
Responsabile Area Cyber Security, Direzione Sicurezza Industriale, SOGIN

Domenico Cuoccio
Responsabile Ufficio Qualità e Sicurezza dei Sistemi Informativi, InnovaPuglia

Carlo Fantini
Dirigente Area Sistemi e Sicurezza, Direzione centrale dei servizi elettorali, Ministero dell'Interno

Massimo Crubellati
Country Manager, Cast Italia

Pasquale Fedele
Responsabile IT CEDA; componente GdL Privacy; referente Dipartimento Sostenibilità per la Privacy, ENEA

Gemma De Angelis
Responsabile Infrastruttura Tecnologia e Esercizio Sistemi - Direzione Centrale Pianificazione, Sistemi, Risorse e Organizzazione, Agenzia del Demanio

Paolo Foschi
Territory Account Manager, Forcepoint

Paolo De Carlo
Deputy Director Aerospace_Defense & Government Markets, Aizoon technology consulting

Leandro Gelasi
Responsabile Settore IT Operations, Corte dei Conti

Marcello Di Monte
Capo sezione studi e coordinamento per lo sviluppo dei sistemi informatici, Segretariato Generale della Difesa Ministero della Difesa

Stefano Giannandrea
Responsabile Area Monitoraggio Qualità & Sicurezza, Lepida

Roberto Guadagni
Responsabile Laboratorio Infrastrutture e Servizi di Rete, ENEA

Diego Mezzina
ICT Security Manager, INSIEL

Roberta Lotti
Dirigente Ufficio II - Direzione dei sistemi informativi e dell'innovazione, Ministero dell'Economia e delle Finanze

Stefano Plantemoli
Responsabile sicurezza IT - Dipartimento per le Politiche del personale dell'amministrazione civile e per le Risorse strumentali e finanziarie, Ministero dell'Interno

Luca Mairani
Sr. Sales Engineer, Forcepoint

Rosario Riccio
Dirigente Ufficio IV - Infrastruttura, rete e sicurezza- D.G. Contratti, Acquisti, Sistemi Informativi e Statistica, Ministero dell'Istruzione, dell'Università e della Ricerca

Antonio Manduca
Divisione ICT, ENEA

Matteo Rigoni
Enterprise Program Manager, Samsung Electronics Italia

Giovanni Mellini
Responsabile del settore Sicurezza delle Informazioni dei Sistemi e delle Reti, ENAV

Marco Romoli
Senior Account Executive, Cast Italia

Ettore Sala
Responsabile Sicurezza Informatica – IT Security Manager, LAZIOCrea Spa

Enzo Veiluva
Responsabile Sicurezza ICT & Privacy, CSI Piemonte

Pierluigi Sartori
Responsabile Cybersecurity, Informatica Trentina

Raffaele Visciano
ICT specialist, Dipartimento delle Finanze, Ministero dell'Economia e delle Finanze

Michele Slocovich
Solution Designer Manager,
Cast Italia

Luca Tricca
Comando Generale - III REP. -
Centro Sicurezza Telematica,
Arma dei Carabinieri

Maurizio Trapanese
Direttore Settore Information
Communication Technology (ICT),
AIFA