#CANTIERI
DELLA PA DIGITALE

SICUREZZA DIGITALE | REPORT 2017

FPA
DIGITAL360

La redazione del report 2017 del Cantiere Sicurezza digitale è stata coordinata da Andrea Ivan Baldassarre, con la supervisione scientifica di Andrea Rigoni.
Il documento costituisce il risultato finale del lavoro collaborativo **tra tutti i protagonisti del Cantiere** svolto nel corso dell'anno.

La sezione principale del report, dal titolo *CERT e Infosharing per la PA: dalla response alla Readiness*, è stata curata da un gruppo di lavoro composto (in ordine rigorosamente alfabetico) da: Giovanni Mellini (Enav), Diego Mezzina (Insiel), Giorgio Mosca (Leonardo), Stefano Plantemoli (Ministero dell'Interno), Andrea Rigoni (Deloitte), Gabriele Rizzo (Leonardo), Pierluigi Sartori (Informatica Trentina), Enzo Veiluva (CSI Piemonte). I due casi di studio sono stati curati da Fabio Lazzini (Sogei) e Monica Pellegrino (ABI-Lab).

Il *focus on* sul tema *PA e mobile security* è stato curato da un gruppo di lavoro composto (in ordine rigorosamente alfabetico) da: Antonio Bosio (Samsung), Fabio Bucciarelli (Regione Emilia Romagna), Gianluca D'Acunzo (GSE - Gestore Servizi Energetici).

CANTIERI DELLA PA DIGITALE
Cantiere Sicurezza digitale - Report 2017 - Edizioni ForumPA - ISBN: 9788897169345

Finito di impaginare: febbraio 2018
con il contributo di:

#CANTIERI
DELLA PA DIGITALE

SICUREZZA DIGITALE | REPORT 2017

FPA
DIGITAL 360

INDICE

L'INIZIATIVA CANTIERI DELLA PA

di **Eleonora Bove**, Content manager, FPA

Le esperienze e le buone pratiche sono in grado, se condivise, di dare un vantaggio competitivo ad ogni organizzazione, compresa la pubblica amministrazione che non a torto è stata definita la più grande azienda del Paese. La chiave del cambiamento sta quindi nel rimettere al centro le persone, le loro conoscenze e relazioni. La *sharing knowledge* genera altra conoscenza ed è proprio questo di cui ha bisogno la nostra PA. Non abbiamo bisogno di norme, quelle ce ne sono anche troppe, ma di **relazioni,** in cui coloro che credono che si possa fare innovazione nella pubblica amministrazione possano trovare un patrimonio cognitivo, competenze e know-how per realizzare azioni concrete di innovazione. Nel 2016 FPA ha lanciato i "Cantieri della PA digitale": **laboratori** in cui i più autorevoli operatori pubblici e privati si sono incontrati per discutere e disegnare i percorsi di attuazione della PA digitale in altrettante aree verticali e trasversali dell'informatica pubblica: cittadinanza, documenti, procurement, scuola, pagamenti, sanità, sicurezza e patrimoni pubblici. Ogni Cantiere opera attraverso un **tavolo di lavoro ristretto** che si riunisce 4 volte all'anno ed esamina lo stato dell'arte del tema; gli ostacoli normativi, di risorse o di comportamenti che rendono problematico il cambiamento; le migliori esperienze italiane e straniere; gli scenari tecnologici più avanzati e le possibilità che questi possono aprire; le modalità di realizzazione dei progetti. Obiettivo: accompagnare lo sviluppo digitale dell'amministrazione italiana, attraverso più canali di confronto e approfondimento, per un sistema più equo e sostenibile.

Con Cantieri PA abbiamo dato vita a rapporti basati su linguaggi e valori comuni che hanno generato nuovi saperi ed esperienze. È stato subito un successo, non scontato per un progetto di questo tipo che voleva mettere insieme soggetti pubblici e professionisti dell'ICT con l'obiettivo di lavorare in modo fattivo e attuale ad una PA più veloce, efficiente e attenta alle esigenze dei cittadini. In parole semplici: una PA in grado di produrre "valore pubblico". Solo dall'azione congiunta di tutte le componenti in gioco: governo, imprese, università e cittadinanza attiva può venire l'innovazione. E l'azione di FPA è proprio quella di favorire la collaborazione tra soggetti diversi, ma

comunemente impegnati a sostenere il cambiamento, perché questo ultimo sia possibile.

All'edizione 2017 hanno preso parte: in totale 250 soggetti, tra cui 200 operatori della PA provenienti da 115 differenti amministrazioni (tra gli altri: 38 grandi enti centrali, 10 Regioni e 20 comuni capoluogo) e i rappresentanti delle 23 aziende partner dei Cantieri.

Siamo usciti dalle sale convegno per entrare in "cantieri" attivi, dove ci rimbocchiamo le maniche e ci apriamo allo scambio di visioni e esperienze. Il segreto sono le relazioni ed una metodologia di lavoro nuova, un format rinnovato a partire dai contenuti, che rispondono ad una domanda operativa: "come" fare innovazione.

Abbiamo dato una struttura alla collaborazione, senza rinunciare a metter insieme soggetti, approcci epistemologici e interessi diversi in un unico momento di lavoro. Che non si esaurisce nei quattro incontri in presenza, previsti per ciascun tavolo, ma che prosegue on line sulla **piattaforma** pensata e progettata da FPA affinché il confronto tra i protagonisti del tavolo e tra questi e la propria comunità di riferimento sia continuo. Questo nuovo spazio virtuale non è soltanto strumento di lavoro a supporto del tavolo negli intervalli temporali tra gli incontri in presenza, ma un vero e proprio spazio di condivisione e confronto tra i diversi operatori della PA centrale e locale responsabili dell'attuazione delle specifiche policy inerenti le varie aree verticali del processo di digitalizzazione della PA.

Unendo il lavoro in presenza e l'attività on line, intorno a ciascun tavolo di lavoro si stanno creando delle vere e proprie **comunità epistemiche**, ovvero network di referenti pubblici accomunati non soltanto da analoghi ruoli formali all'interno delle rispettive amministrazioni, ma anche e soprattutto dalla condivisione di expertise, conoscenze e valori comuni rispetto ai processi di innovazione della PA: dai responsabili dello sviluppo dei servizi online per cittadini e imprese, ai referenti dei progetti di dematerializzazione e gestione documentale; dai coordinatori della sicurezza informatica degli enti centrali e locali, ai responsabili dell'innovazione dei processi di approvvigionamento della PA; dai protagonisti dei progetti di innovazione degli ambienti di apprendimento nella Scuola, a quelli relativi alla digitalizzazione del Sistema Sanitario Nazionale.

Le community dei Cantieri si configurano quindi come **laboratori multidisciplinari permanenti.** Un lungo percorso di analisi e condivisione, aperto e interattivo, in cui le politiche vengono esaminate con i tanti punti di vista coinvolti, abbattendo le linee che separano in silos ogni ufficio, ente, processo per far uscire problematiche diffuse e ostacoli a cui trovare, insieme, le soluzioni.

IL COMMENTO AL 2017

UN ANNO CALDO PER LA SICUREZZA INFORMATICA, MA LA PA FA ANCORA FATICA[1]

di **Andrea Rigoni**, Partner Cyber Security - Deloitte Risk Advisory - Advisor del Cantiere Sicurezza digitale

Anche il 2017 si è confermato un anno molto caldo per la Cyber Security nel nostro paese. Numerosi sono stati gli avvenimenti sia dal punto di vista degli attacchi e delle minacce, sia da quello regolatorio e normativo.

Il 2017 è stato l'anno degli attacchi su vasta scala, che hanno creato parecchio clamore sulla stampa e sui media. Quello più noto è senz'altro **WannaCry**, un attacco di tipo "ransomware" che ha colpito 99 paesi, tra cui l'Italia. Un codice malevolo creato con materiale sottratto al governo americano che, una volta infettato un PC, procedeva alla cifratura di tutti i dati rendendoli indisponibili. Nonostante il clamore, le grandi aziende e i governi che hanno sofferto danni ingenti sono stati relativamente pochi. WannaCry è stato poi seguito da altri attacchi come **Petya** (o NotPetya/Nyetya/ExPetr, come alcuno lo hanno poi ribattezzato), una evoluzione dello stesso WannaCry: qui i danni sono stati concentrati in Ucraina, in particolare in grandi banche, compagnie elettriche, società di trasporti e persino la centrale nucleare di Chernobyl. Insomma, un anno tra i più "caldi" della storia, anche se la portata degli attacchi non ha di certo stupito gli esperti che in più occasioni hanno ribadito che i danni avrebbero potuto essere di gran lunga superiori, viste le vulnerabilità dei sistemi e la sofisticatezza delle tecniche di attacco impiegate.

Una fotografia di costante aumento delle minacce è stata data anche dalla relazione annuale al parlamento sulla sicurezza della Repubblica 2016, pubblicata il 27 febbraio 2017, nella quale si legge: "la dimensione cibernetica della minaccia [è] in grado di produrre effetti di estrema gravità fino alla paralisi di settori vitali del Paese".

Il 13 aprile 2017 viene pubblicato sulla Gazzetta Ufficiale n. 87 il Decreto del

[1] Questo articolo è tratto dall'*Annual Report 2017* di FPA

Presidente del Consiglio dei Ministri del 17 febbraio 2017 contenente la "**Direttiva recante indirizzi per la protezione cibernetica e la sicurezza informatica nazionali**". Si tratta di una revisione evolutiva del precedente DPCM del 24 gennaio 2013 che, oltre a rafforzare il ruolo di coordinamento del Dipartimento delle Informazioni per la Sicurezza (DIS) presso la Presidenza del Consiglio dei Ministri, introduce una serie di indicazioni per gli operatori privati (art. 11).

Il 31 maggio 2017 viene pubblicato sulla Gazzetta Ufficiale n. 125 il Decreto del Presidente del Consiglio dei Ministri del 31 marzo 2017 contenente il nuovo "**Piano Nazionale per la protezione Cibernetica e la sicurezza informatica Nazionale**", andando a sostituire quello pubblicato nel febbraio del 2014. Con il nuovo decreto viene istituito il **Nucleo di Sicurezza Cibernetica** presso il DIS, con compiti di coordinamento della risposta ad attacchi di rilevanza nazionale. Inoltre, i CERT istituiti presso il MISE (CERT Nazionale) e AgID (CERT PA) dovranno andare a convergere in modo da massimizzare la sinergia e lo sfruttamento delle risorse.

In questo quadro, vanno anche ricordati i due interventi normativi dell'Unione Europea, che hanno avuto effetti sulle strategie sia nazionali che degli operatori privati. Il 4 maggio 2016 è stato pubblicato in Gazzetta Ufficiale Europea il ***General Data Protection Regulation (GDPR)***, entrato in vigore il 25 maggio dello stesso anno e con efficacia dal 25 maggio 2018. Il 6 luglio 2016 vi è stata l'adozione della Direttiva UE 2016/1148, recante "misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione" (c.d. **Direttiva NIS - *Network and Information Systems***). L'approvazione di tale Direttiva, che dovrà essere recepita nell'ordinamento nazionale entro il maggio 2018, ha fornito lo spunto per indirizzare ulteriormente gli atti di indirizzo strategico e operativo (Quadro Strategico e Piano Nazionale).

Altro evento italiano degno di nota è la creazione del **CERT-FIN**, ovvero del CERT del settore finanziario, istituito presso ABI-LAB con il supporto e la partecipazione di tutte le più grandi banche Italiane. Si tratta di un importante passo verso l'evoluzione di partnership pubblico private finalizzate a una cooperazione e collaborazione fattuale e operativa, basata sullo scambio di informazioni e sulla messa a fattor comune di competenze e di esperienze, anche provenienti da altri settori e da altri paesi. Sempre nell'ambito finanziario va menzionato il **progetto OF2CEN**, partito dall'Italia nel 2011 per opera del Ministero dell'Interno/Polizia Postale e delle Comunicazioni e finalizzato alla creazione di una rete sicura di scambio di informazioni tra attori del settore finanziario e forze dell'ordine. Finanziato dall'Unione Europea, il progetto è giunto ora alla sua seconda versione, con il coinvolgimento di Europol e di forze dell'ordine di altri paesi europei. Il progetto a DNA Italiano è stato menzionato come caso di successo nella Comunicazione Congiunta del

Parlamento Europeo e del Consiglio su "**Resilienza, Deterrenza e Difesa: verso una cibersicurezza più forte per l'UE**".

Nonostante la costante evoluzione dell'attenzione sia mediatica che istituzionale al tema della Cybersecurity, le iniziative di miglioramento dei presidi di sicurezza fanno fatica a decollare, in particolare nella pubblica amministrazione, dove si continua a registrare uno stato di semi-immobilismo, se paragonato a quello del settore privato, in particolare degli operatori di servizi essenziali (quali banche, aziende elettriche e trasporti). Nella Pubblica Amministrazione persiste una grande difficoltà nell'avviamento di progetti e nella costruzione di modelli adeguati di gestione della sicurezza. Nonostante gli sforzi profusi dalle istituzioni, e in particolare l'Agenzia per l'Italia Digitale, le amministrazioni non dispongono ancora di un apparato organizzativo e di responsabilità che consenta una agile adozione delle misure minime e dei processi chiave della sicurezza. La situazione peggiora in modo proporzionale alle dimensioni dell'amministrazione: se le grandi amministrazioni centrali, insieme ad alcune amministrazioni regionali, hanno avviato piani e iniziative di miglioramento della propria sicurezza, le amministrazioni più piccole fanno una enorme fatica a trovare le leve e le risorse, anche perché spesso mancano figure che sentano propria la responsabilità della *cybersecurity*. In realtà, è già responsabilità chiara degli amministratori il dover proteggere i propri dati e i propri servizi, ma è necessaria una opera forte di educazione e sensibilizzazione, insieme alla fornitura di strumenti operativi semplici e chiari per agevolare il loro compito.

CERT E INFOSHARING PER LA PA: DALLA *RESPONSE* ALLA *READINES*

INTRODUZIONE: PERCHÉ UN REPORT SUI CERT

di **Andrea Ivan Baldassarre**, Project Manager Cantieri della PA, FPA

Già nel corso della sua prima edizione, il Cantiere sulla Sicurezza digitale aveva evidenziato la rinnovata attenzione verso il tema dei CERT (*Computer Emergency Response Team*) e del ruolo che questi possono svolgere nello sviluppo di capacità avanzate di rilevazione e risposta ad incidenti informatici nel settore pubblico.

Un'attenzione motivata dalla spinta impressa dall'Unione Europea, che da anni promuove l'adozione dei CERT nelle organizzazioni pubbliche e private come uno degli elementi fondamentali della propria strategia sulla cybersecurity, e che con l'adozione della Direttiva NIS - *Network and Information Security* (2016), ha posto le basi per lo sviluppo di strutture in grado di garantire adeguate la capacità di risposta e prevenzione agli eventi cibernetici in tutti i Paesi membri.

La Direttiva NIS, che dovrà essere recepita nell'ordinamento nazionale entro il maggio 2018, ha fornito lo spunto per indirizzare ulteriormente gli atti di indirizzo strategico e operativo (Quadro Strategico e Piano Nazionale), in particolare per ciò che attiene l'operatività delle strutture nazionali di *incident prevention, response e remediation*.

Non è infatti un caso che le maggiori novità introdotte dalla nuova versione del **Piano Nazionale per la protezione cibernetica e la sicurezza informatica**, approvato a marzo 2017 in attuazione del c.d. DPCM Gentiloni[2], si siano concentrate sull'Indirizzo Operativo 5, nel quale si riconosce che "l'approntamento di capacità di prevenzione e reazione ad eventi cibernetici richiede lo sviluppo di *Computer Emergency Response Team* (CERT) quali soggetti erogatori di servizi di assistenza tecnica, ricerca e sviluppo, formazione e informazione per i rispettivi utenti, pubblici e/o privati". Eppure si registra ancora oggi una certa carenza di linee guida e documenti di indirizzo su come rea-

[2] DPCM 17 febbraio 2017, *Direttiva recante nuovi indirizzi per la protezione cibernetica e la sicurezza informatica*

lizzare tali strutture all'interno delle pubbliche amministrazioni, e non solo. Le principali linee guida esistenti sono infatti state pubblicate dal Software Engineering Institute della Carnegie Mellon University (luogo di nascita dei CERT), e da ENISA, l'Agenzia europea per la sicurezza delle reti e dell'informazione[3]. Ma come sottolineato da Andrea Rigoni, coordinatore del Cantiere, *"si tratta di linee guida generiche adatte a qualsiasi settore. Non trattano però le specificità della situazione Italiana, in particolare il modello organizzativo interno, le capabilities di base e la relazione con le altre strutture istituzionali"* [4].

Già nel 2016, il Cantiere aveva suggerito la necessità che AgID realizzasse delle linee guida su come costituire un CERT, che indicassero alle pubbliche amministrazioni i vari passi da seguire e i principali elementi cui prestare attenzione per realizzare un *Computer Emergency Response* (o meglio *Readiness*) *Team*, integrando indicazioni operative con alcuni esempi riferiti a *best practice* riconosciute a livello nazionale e internazionale.

Da qui l'idea di dedicare il percorso di analisi del 2017 alla definizione di un nucleo fondamentale di indicazioni utili allo sviluppo di un'ipotetica linea guida sui CERT della PA e sulle relative attività di *information sharing*, considerate come il fondamentale catalizzatore per l'avvio di un sistema di collaborazione tra CERT. Una sorta di "abecedario" degli elementi organizzativi, tecnologici e procedurali di cui si dovrebbe tener conto nel processo di costituzione di un CERT/CSIRT, da sottoporre ad AgID per la loro validazione e distribuzione.

[3] *Un approccio graduale alla creazione di un CSIRT*, ENISA, 2006

[4] **Cosa sono i CERT: ecco le risposte ai vostri dubbi**

SEZIONE 1: CSIRT E CERT

a cura di: **Diego Mezzina** (Insiel), **Giorgio Mosca** (Leonardo), **Andrea Rigoni** (Deloitte), **Gabriele Rizzo** (Leonardo), **Pierluigi Sartori** (Informatica Trentina), **Enzo Veiluva** (CSI Piemonte)

IL CONTESTO NORMATIVO: IL CSIRT ALL'INTERNO DELLA NORMATIVA NIS E NEL PIANO NAZIONALE DI SICUREZZA

L'importanza strategica dei CERT nel garantire la capacità di prevenzione e reazione agli eventi cibernetici è da tempo riconosciuta anche dal Governo italiano, che aveva già dedicato uno specifico indirizzo operativo al tema nel Piano Nazionale per la Protezione Cibernetica e la Sicurezza Informatica del 2013. L'Indirizzo Operativo 5, oltre ad affidare una rilevanza cruciale allo sviluppo del CERT-PA (Obiettivo Specifico 5.1, Linea d'azione a) e all'avvio del CERT Nazionale (Obiettivo Specifico 5.2), annoverava tra le azioni da intraprendere:

- la creazione di un *"sistema di cooperazione delle strutture di gestione della sicurezza ICT della PA, in particolare Unità Locali di Sicurezza (ULS) e Security Operations Center (SOC), promuovendone, ove possibile, la trasformazione in CERT dicasteriali"* (Obiettivo Specifico 5.1, Linea d'azione b);
- la *"creazione di CERT Regionali con il compito di supportare le Pubbliche Amministrazioni Locali (PAL) del territorio e di implementare regole e modelli organizzativi nazionali"* (Obiettivo Specifico 5.1, Linea d'azione c).

Nell'aggiornamento di maggio 2017 del Piano Nazionale sempre all'Indirizzo Operativo 5, si ribadisce che *"L'approntamento di capacità di prevenzione e reazione ad eventi cibernetici richiede lo sviluppo di Computer Emergency Response Team (CERT) quali soggetti erogatori di servizi di assistenza tecnica, ricerca e sviluppo, formazione e informazione per i rispettivi utenti, pubblici e/o privati. La Direttiva NIS prevede, quantomeno a favore dei gestori di servizi essenziali, la costituzione dei CERT* (che però vengono definiti CSIRT, Computer Security Incident Response Team)*, designazione preferita dalle autorità Europee poiché CERT è un marchio registrato della Carnegie Mellon University. In questo documento CERT e CISRT verranno utilizzati in modo equivalente. Nel contesto del recepimento delle novità introdotte dalla Direttiva NIS, occorre ridefinire il ruolo*

rivestito dagli attori presenti nell'attuale architettura nazionale (i vari CERT) e quelli che vi faranno ingresso (oltre a CSIRT, Autorità nazionale/i e punto unico di contatto). Nelle more del recepimento della direttiva NIS, sarà avviato un processo di progressiva unificazione dei CERT pubblici per sancire, nei settori di interesse strategico, la competenza esclusiva di un CERT nazionale unico, ovvero per creare una rete nazionale di CERT individuando un soggetto con poteri di coordinamento".

L'obiettivo di questo documento è quello di delineare il ruolo e le responsabilità che potrebbero ricoprire le organizzazioni territoriali che hanno istituito al loro interno dei Security Operation Center o dei CERT. Difatti le pubbliche amministrazioni e le aziende locali da tempo cercano di creare maggiori competenze e servizi specialistici per contrastare le minacce cibernetiche che di anno in anno crescono in numero e sofisticatezza, ma non tutte possiedono dimensioni, risorse umane ed economiche sufficienti per raggiungere il risultato, né rientrare nel loro core business. La possibilità di appoggiarsi su infrastrutture specializzate che svolgono funzioni di CSIRT Territoriali di riferimento gioverebbe moltissimo all'innalzamento dei livelli di sicurezza di tali aziende /enti.

Queste infrastrutture hanno **le competenze e capacità per puntare alla realizzazione di CERT locali che svolgano funzione di raccordo e cooperazione sulla sicurezza per tutti gli Enti pubblici presenti nei territori di propria competenza** in modo da poter far fronte ad attacchi portati su una scala sempre più vasta. È importante però, se si vuole giungere a questi risultati che le strutture possano godere degli accreditamenti necessari, tanto a livello locale, quanto a livello nazionale e internazionale, fornendo il monitoraggio e l'assistenza agli utenti della propria comunità di riferimento, nell'attuazione di misure proattive per ridurre i rischi di incidenti di sicurezza informatica e nella risposta (misure reattive) a tali incidenti, in collaborazione con i CERT pubblici del Governo. Per tale scopo si delineano nella seconda parte di questa sezione del documento una serie di linee guida che possano essere di riferimento anche per AGID, nell'identificazione dei requisiti necessari e di suggerimenti sull'approccio metodologico e tecnico da seguire

IL RUOLO DEL CERT: IL CERT COME *CAPABILITY* E DIFFERENZA CON ALTRE STRUTTURE PREPOSTE ALLA SICUREZZA INFORMATICA

La creazione dei CERT è una pratica adottata da molti Paesi e da molti settori per avviare capacità avanzate di rilevazione e risposta ad incidenti informatici. Come noto, il suo ruolo principale consiste nel coordinare, supportare e monitorare le attività di prevenzione, risposta e ripristino degli incidenti critici di tipo cyber, abilitando e coordinando le comunicazioni interne ed esterne e supportando la conformità a standard e normative di riferimento, per consentire il rapido ed efficace ripristino dell'operatività sulla base di regole

e procedure già definite da attivare in risposta all'attacco. In questo senso il CERT si sta affermando, sia nel mondo pubblico, sia in quello privato, come il punto di contatto principale per la difesa dalla minaccia cyber. Da anni L'Unione Europa promuove l'adozione dei CERT/CSIRT nelle organizzazioni pubbliche e private come uno degli elementi fondamentali della propria strategia sulla *cybersecurity*. Un'attenzione ribadita nell'adozione della Direttiva NIS (Network Information Security), che dedica particolare attenzione al tema.

La direttiva, almeno in base a quanto esposto nelle intenzioni del legislatore comunitario, sostiene l'istituzione dei CERT come una vera e propria necessità strategica, l'unica in grado di garantire: 1) la notifica degli incidenti all'autorità nazionale responsabile; 2) la corretta gestione degli incidenti che, indipendentemente dall'etichetta, i fornitori di servizi essenziali sono chiamati a garantire. Oltre al focus sulla rilevazione e risposta agli incidenti informatici, i CERT costituiscono una capacità di valore per la *constituency* anche in relazione alla **prevenzione degli incidenti**, e all'aumento della cultura della sicurezza. Infatti, il modello di riferimento per i CERT, ovvero l'*Handbook of Computer Security Incident Response Teams*, prevede che un CERT possa erogare una gamma di servizi completa e strutturata, di cui la gestione degli incidenti è parte integrante.

In tal senso più che di *Response* (risposta) si tende a parlare di *Readiness* (prontezza / preparazione), in quanto con l'evoluzione dei servizi informatici e l'aumento dei relativi rischi, ogni Organizzazione/Ente si trova alle prese con gli incidenti informatici deve quindi prepararsi per tempo, sviluppando la propria cultura e mettendo in campo azioni proattive e procedure, per ridurre la probabilità ma anche l'impatto degli incidenti.

Il mix di servizi erogato da un CERT lo può distinguere e rendere complementare ad altre strutture di gestione della sicurezza, che, se concentrate su una parte delle *capabilities* (cultura, prevenzione, reazione) o verticalizzate su un servizio o focalizzate su una parte dell'infrastruttura, possono avere più difficoltà nella produzione di valore per la *constituency*.

Un CERT può invece qualificarsi per la sua constituency come punto di riferimento per l'evoluzione del modello di sicurezza ed il raggiungimento di livelli omogenei, soprattutto in scenari dove i singoli attori possono non disporre delle risorse necessarie a sviluppare adeguate capacità (come nel caso della PAL).

Servizi erogabili da uno CSIRT, secondo SEI-CMU (Handbook of CSIRTs)

Reactive Services	Proactive Services	Security Quality Management Services
Alerts and Warnings Incident Handling – Incident analysis – Incident response on site – Incident response support – Incident response coordination Vulnerability Handling – Vulnerability analysis – Vulnerability response – Vulnerability response coordination Artifact Handling – Artifact analysis – Artifact response – Artifact response coordination	Announcements Technology Watch Security Audits or Assessments Configuration and maintenance of Security Tools, Applications, and Infrastructures Development of Security Tools Intrusion Detection Services Security-Related Information Dissemination	Risk Analysis Business Continuity and Disaster Recovery Planning Security Consulting Awareness Building Education/Training Product Evaluation or Certification

Questa potenzialità consente, ai suddetti enti, di:

- avere un coordinamento centralizzato per le questioni di sicurezza al fine di garantire una gestione ed una risposta centralizzata e specializzata agli incidenti IT;
- avere immediatamente disponibile la competenza per sostenere e aiutare gli utenti a riprendersi rapidamente dagli incidenti di sicurezza;
- trattare gli aspetti giuridici e conservare la documentazione nel caso di un'azione legale;
- tenersi al corrente degli sviluppi nel campo della sicurezza;
- stimolare la cooperazione all'interno della comunità di riferimento in merito alla sicurezza IT (sensibilizzazione).

DIFFERENZA TRA CERT DI SETTORE, CERT DICASTERIALI E CERT TERRITORIALI

Se si analizza la Direttiva NIS, al considerando (34) viene indicato che: "È opportuno che gli Stati membri siano dotati delle capacità tecniche e organizzative necessarie a prevenire, individuare, rispondere e attenuare i rischi e gli incidenti a carico delle reti e dei sistemi informativi. Gli Stati membri dovrebbero pertanto assicurare la disponibilità di CSIRT, anche noti come squadre di pronto intervento informatico («CERT»), ben funzionanti e rispondenti a determinati requisiti essenziali, in modo da garantire l›esistenza di capacità effettive e compatibili per far fronte ai rischi e agli incidenti e garantire un›efficiente collaborazione a livello *di Unione. Per consentire a tutti i tipi di operatori di servizi essenziali e forni-*

tori di servizi digitali di beneficiare di tali capacità e cooperazione, gli Stati membri dovrebbero assicurare che tutti i tipi siano contemplati da un CSIRT designato. Data l'importanza della cooperazione internazionale in materia di cibersicurezza, i CSIRT dovrebbero poter partecipare a reti di cooperazione internazionale oltre alla rete di CSIRT istituita dalla presente direttiva."

Alla luce di queste e altre considerazioni distribuite all'interno del testo della direttiva, appare evidente che, affinché il sistema di gestione degli *alert* e di raccolta delle informazioni su attacchi informatici (*infosharing*) possa essere condotto in maniera efficace, occorre una rete interna ad ogni stato membro in stretta e forte collaborazione con le diverse tipologie di aziende e pubbliche amministrazioni presenti sul territorio nazionale. Oggi, oltre alle realtà di CERT Nazionale e CERT PA, che progressivamente dovrebbero vedere una loro unificazione, sono presenti sul territorio molteplici istituzioni di CERT di ampia portata, pubblici e privati, quali CERTfin (CERT del settore Bancario, gestito da ABIlab in congiunzione con Banca d'Italia), Poste Italiane, Sogei, il GARR, la Regione Autonoma Friuli Venezia Giulia, solo per citare alcuni esempi. È importante quindi che a livello di definizione di linee guida vengano assolutamente prese in considerazione le modalità di interazione tra le varie realtà del territorio.

Non è semplice definire differenze o ruoli specifici legati alle diverse tipologie di CERT oggi presenti, e forse non è molto sensato pensare a compartimentazioni di attività svolte da CERT di settore, dicasteriali o territoriali. Se si prendono in considerazioni, solo per fare qualche esempio concreto, attacchi mirati alla compromissione di sistemi e reti attraverso la diffusione di malware per finalità di estorsione o inserimento in *botnet*, tutte le realtà aziendali pubbliche e/o private possono essere considerate a rischio, mentre per quanto riguarda, ad esempio, le minacce dovute all'hactivism, potrebbe esserci uno sbilanciamento più rivolto verso le pubbliche amministrazioni (ma ciò non e sempre detto, dipende molto anche dalle circostanze). In alcuni casi, l'eventuale differenza potrebbe essere dovuta al tipo di tecnologie impiegate, da cui derivano di conseguenza raccolte diversificate di sfruttamento di vulnerabilità. Potenzialmente, CSIRT dedicati al monitoraggio delle Pubbliche amministrazioni potrebbero avere una maggiore evidenza di tentativi di sfruttamento di vulnerabilità presenti in soluzioni *open source*, rispetto al mondo privato. Ciò non incide comunque su una differenziazione di processi e responsabilità che rimane invece uniforme.

Nella costituzione del rapporto di collaborazione tra le varie realtà, le istituzioni governative centrali (CERT PA e NAZIONALE) devono sicuramente giocare un ruolo di riferimento principale nella rete nazionale ed europea, verso i quali le varie realtà locali devono interagire, creando delle reti di correlazione, ma soprattutto di divulgazione e supporto in caso di incidente territoriale.

I CERT TERRITORIALI E AUTONOMIE LOCALI E RUOLO DELLE IN HOUSE ICT. QUALI INTERAZIONI?

I centri di difesa territoriali oggi presenti nelle singole in-house sono ancora troppo focalizzati sulla protezione interna dell'organizzazione (intesa come l'organizzazione dell'azienda in-house stessa e del sistema regionale a cui fanno riferimento) e non nascono con un vero e proprio spirito di cooperazione tra di esse, aspetto cruciale per attuare quanto previsto dal Piano Nazionale. Inoltre, vi è il rischio che alcune aziende in-house non abbiano sviluppato sufficienti capacità di protezione di sicurezza cibernetica. Infine, anche qualora esse siano dotate di capacità avanzate, c'è il rischio che queste siano disallineate con quelle di altre amministrazioni, di fatto rendendo impossibile o inefficace una difesa di sistema. Ad oggi, vi sono diversi ostacoli che non facilitano l'evoluzione di questi centri di competenza e monitoraggio della sicurezza verso un approccio CERT. Tra tali elementi si possono identificare: la scarsità dei budget destinati alla sicurezza informatica che, almeno sulla base dei vincoli della Direttiva, dovrebbe auspicabilmente migliorare in futuro; la mancanza di regole tecniche e standard omogenei per uniformare finalità e capacità richieste ai diversi CERT; l'insufficienza di esperienze e competenze di condivisione di scelte tecnologiche e framework comuni di interscambio delle informazioni. Il superamento di tali elementi non può prescindere dalla più ampia consapevolezza e senso di urgenza associato al recepimento della Direttiva e, più nello specifico, degli indirizzi operativi contenuti nel Piano Nazionale, con l'obiettivo di contrastare e ridurre, almeno in parte, i rischi crescenti legati alla minaccia cibernetica.

L'approccio che ne potrebbe derivare comporterebbe sicuramente dei vantaggi a livello di miglioramento del monitoraggio della sicurezza sull'intero territorio nazionale. Le ricadute attese a livello locale comporterebbero:

- un governo guidato dal centro per le questioni di sicurezza al fine di garantire una gestione ed una risposta efficace e specializzata agli incidenti di sicurezza cibernetica;
- la possibilità di scalare rapidamente un incidente locale in modo da pre-allertare l'intera pubblica amministrazione o quantomeno quelle amministrazioni che potrebbero subire attacchi simili;
- favorire la cooperazione tra amministrazioni (locali e centrali), istituzioni di sicurezza nazionale e operatori di mercato in modo di massimizzare l'efficacia delle risposte agli incidenti e la loro prevenzione;
- un contributo alla definizione ed al raggiungimento di livelli di sicurezza omogenei, proponendo livelli minimi di sicurezza coerentemente con le best practice e in linea con i vincoli derivanti dalla normativa cogente.

Il valore che le in-house, in particolare quelle a carattere strumentale per la gestione dei sistemi informativi delle PA, su tali fronti possono apportare è notevole. Difatti, nella maggior parte delle in-house è definita una politica della sicurezza che prevede, da un lato, la predisposizione di architetture per la condivisione del patrimonio informativo, l'interoperabilità, la cooperazione tra applicazioni, l'automazione dei processi amministrativi e dall'altro, l'autonomia di ogni settore di intervento per il proprio ambito. In questo scenario la sicurezza risulta strategica per garantire l'affidabilità dei processi, dei dati elaborati e dei servizi resi al cittadino.

In particolare, le in-house attuano già obbiettivi sul versante dei servizi alle pubbliche amministrazioni, che contribuiscono a fornire:

- servizi di analisi e di indirizzo, finalizzati a supportare la definizione dei processi di gestione della sicurezza, lo sviluppo di metodologie, il disegno di processi e di metriche valutative per il governo della sicurezza cibernetica;
- servizi proattivi, aventi come scopo la raccolta e l'elaborazione di dati significativi ai fini della sicurezza cibernetica, l'emanazione di bollettini e segnalazioni di sicurezza, l'implementazione e la gestione di basi dati informative;
- servizi reattivi, aventi come scopo la gestione degli allarmi di sicurezza, il supporto ai processi di gestione e risoluzione degli incidenti di sicurezza all'interno del dominio delle PA;
- servizi di formazione e comunicazione per promuovere la cultura della sicurezza cibernetica, favorendo il grado di consapevolezza e competenza all'interno delle PA, attraverso la condivisione di informazioni relative a specifici eventi in corso, nuovi scenari di rischio o specifiche tematiche di sicurezza delle informazioni;
- servizi di protezione vera e propria, o erogati centralmente, o sulla base di regole di sicurezza omogenee: ad esempio sistemi di protezione antimalware centralizzati, sistemi di protezione della navigazione web e della posta elettronica, basati su tecnologie all'avanguardia gestite da personale competente, che contribuiscono sia all'effettiva mitigazione dei rischi di sicurezza, sia alla conformità ai dettami normativi, quali ad esempio le misure minime di sicurezza ICT per la PA emesse dall'AgID;
- servizi di sensibilizzazione alle tematiche della sicurezza delle informazioni, ad esempio attraverso l'erogazione di pillole formative, la stesura di vademecum, il supporto consulenziale ai vari livelli, operativi e decisionali.

In tale contesto, le in-house si configurano, per dimensioni, competenze e posizionamento, come il naturale supporto alla Regioni per diventare punto di riferimento e di contatto con il territorio, in relazione all'adozione delle best practice di settore e dei vincoli derivanti dalla normativa cogente.

Hanno infatti dimensioni sufficienti per sviluppare, a fronte di opportuni budget, capabilities adeguate, ma non eccessive da perdere il contatto con le peculiarità del territorio servito, in termini di opportunità ma anche di criticità.

LINEE GUIDA SUI CERT

Aspetti organizzativi

Diversi sono i riferimenti in letteratura a principali standard, linee guida e best practice adottati per la realizzazione e la conduzione funzionale di un CSIRT:

- CERT Cooperation Center – *Handbook for Computer Security Incident Response Team*;
- European Network and Information Security Agency – *Un approccio graduale alla creazione di un CSIRT*;
- Forum of Incident Response and Security Teams – *FIRST Best Practice Guide Library*;
- Internet Engineering Task Force – *RFC2350, Expectations for Computer Security Incident Response;*
- National Institute for Standards and Technology – *Computer Security Incident Handling Guide, SP800-61*;
- International Organization for Standardization – *Information Security Incident Management ISO/IEC 27035:2011*;
- Asia Pacific CERT – *Guidelines for APCERT POC Arrangements*.

Le principali esperienze di successo hanno dimostrato però che senza l'approvazione e il supporto dei vertici dell'organizzazione, la creazione di una capacità di risposta agli incidenti efficace può essere estremamente difficile e problematica. Questo supporto deve concretizzarsi in vari modi, compresa la fornitura di risorse, finanziamenti e tempo al team di progetto che cura l'implementazione di un CERT. Ciò include anche i dirigenti esecutivi e aziendali o dei dipartimenti e il loro personale che si impegnano a partecipare a questo processo di pianificazione, sia nelle fasi di predisposizione che nelle successive fasi di mantenimento del servizio. Questo è un vincolo fondamentale per il successo dell'operazione, ma può essere non sufficiente in quanto i costi fissi, tanto in termini economici quanto di *effort*, legati alla costituzione di un CSIRT restano, in termini assoluti, rilevanti se non ripartiti tra un adeguato numero di stakeholder.

Per rispondere ai due problemi principali legati alla costituzione di un CERT – gli alti costi fissi e la carenza di risorse specializzate – una soluzione percorribile, già intrapresa da alcune realtà territoriali nazionali, è quella di costituire gruppi di lavoro estesi, ai quali partecipano, insieme alle in-house (cui spetta un ruolo di coordinamento di tali gruppi), i diversi rappresentanti

delle PAL (Comuni, Province, Regioni, altre in-house di settori diversi dall'IT), i rappresentanti del sistema universitario e del mondo della ricerca, le aziende sanitarie nonché, quando identificati, gli operatori di servizi essenziali così come previsto dalla Direttiva NIS.

I vantaggi di questo approccio sono molteplici:

- ampliando la platea diminuisce, ovviamente, la quota parte di costi fissi a carico di ogni ente, con un incremento minimo dei costi variabili dovuti alla gestione di categorie di soggetti eterogenee;
- le competenze presenti sul territorio – o formate secondo necessità – diventano un patrimonio comune a tutti i soggetti interessati, scoraggiando anche un potenziale *turnover* delle stesse da un CSIRT all'altro;
- il patrimonio informativo di conoscenze viene messo a fattor comune. In questo modo si favorisce una più pronta risposta ad eventuali incidenti grazie anche alla possibilità di coordinare i vari soggetti da un un'unica regia. Tale aspetto assume una rilevanza maggiore nel caso di attacchi non mirati e ad ampio spettro.

Possibili percorsi di costruzione di un CERT territoriale

Molte delle strutture locali, candidabili a CERT Locali oggi hanno principalmente due strutture di monitoraggio sicurezza: il NOC ed il SOC. Come suggerisce la parola stessa, un ***Network Operation Center*** è quel luogo composto da persone e da strumenti automatizzati avente come obiettivo il monitoraggio dell'infrastruttura IT, come per esempio (ma non limitato a): Bandwidth, stato aggiornamento firmware, consumo disco, consumo CPU, consumo RAM sui principali assets informatici societari, verifica backup periodico, verifica strumenti e procedure per un disaster recovery, verifica consumi energetici datacenter, ecc.

In modo complementare, un ***Security Operation Center*** è un luogo composto da persone e da strumenti avente come obiettivo il mantenimento dei dispositivi di sicurezza, come per esempio (ma non limitato a): mantenimento regole IPS/IDS, aggiornamenti status dei firmware id firewall, mantenimento ed aggiornamento regole di Proxies e regole di Firewalling, esecuzione dei vulnerability assessment periodici sui principali asset societari, gestione delle rispettive patches, controllo sullo status di update per ogni sistema client e distribuzione dell'aggiornamento.

I primi passi verso un gradino superiore di evoluzione del SOC dovrebbe essere quello di eseguire al proprio interno piccoli e semplici processi attribuibili ad un CERT. Un classico approccio verso tale funzione potrebbe essere quello di affidare la gestione di tutti i segnali (vedi i log) provenienti dai sistemi perimetrali - come per esempio (ma non limitato a) Firewall, IPS, IDS,

AntiVirus, AntiSpam, AntiPhising, ecc. - ad un sistema accentratore denominato SIEM.

Alcuni SIEM (per correttezza non verranno nominati i produttori) sono più idonei di altri per la realizzazione di un SOC avanzato, in quanto possiedono al loro interno il processo necessario per la presa in carico di un incidente e per la sua relativa gestione.

Contrariamente, altri SIEM sono più idonei alla realizzazione di Log Management ove un incidente di sicurezza deve poter essere "ricercato" ma non necessariamente gestito e/o analizzato.

Oltre a piattaforme tradizionali di SIEM, le tecnologie abilitanti e i processi a supporto della *Cyber Detection & Response* dovrebbero essere integrati con strumenti in grado di incrementare le capacità di "*Threat Hunting*" non basati esclusivamente sulla *real time detection* per l'identificazione di incidenti di sicurezza ma anche su analisi storiche di eventi e correlazione di fonti diverse. Piattaforme di *Security Analytics* e di *User & Entity Behaviour Analysis*, accompagnati dalla creazione e gestione di *Security Big Data Lake*, possono incrementare notevolmente le capacità di identificare eventi e incidenti di sicurezza, utilizzando algoritmi comportamentali e tecniche di *machine learning*.

Anche le capacità di automatizzare la risposta ad incidenti di sicurezza diventano un fattore determinante per migliorare la qualità di risposta (evitando, laddove possibile, gli errori umani) e ridurre i tempi di risposta ad Incidenti di Cyber Security. Ciò è possibile grazie a piattaforme e processi di *Security Automation & Orchestration* che integrandosi alla infrastruttura di Prevention (Firewall, IPS, etc) riescono ad attivare delle regole di contenimento (es: blocco IP, blocco sender email a fronte di phishing accertato, ecc..) sulla base si eventi specifici.

Il CERT, a differenza del SOC, è bilanciato tra mondo esterno e interno, rappresentando il principale riferimento per gli aspetti di Cyber Security verso la propria comunità interna (cosiddetta "Constituency") e tutti gli altri attori esterni, istituzionali e non, impegnati quotidianamente nel contrasto e nella difesa del cyber space (altri CERT, forze di polizia, enti regolatori, ecc.). Alla base di questo paradigma vi è lo scambio informativo sulle minacce, sugli incidenti già accaduti e sulle tecniche di contrasto adottate, conosciuto dagli addetti ai lavori come *information sharing* (vedi sezione 2). D'altra parte, è la stessa tecnica di base utilizzata dalle organizzazioni criminali, seppure con modalità e strumenti diversi, per scambiarsi informazioni tecniche aggiornate su come e quando attaccare le vittime, spesso proprio sfruttando le potenzialità della Rete.

Ma per permettere di effettuare questo passaggio da NOC/SOC a CERT, nascono spontanei questi interrogativi:

- Che tipo di servizi dovrebbero essere offerti?
- Quanto dovrebbe essere grande un CERT territoriale?
- Dove dovrebbe essere collocato un CERT nell'organizzazione dell'in-house?
- Quanto costerà implementare e supportare una squadra?
- Quali sono i passi iniziali da seguire per creare un CERT?

Non esiste una sola risposta a queste domande. I CERT territoriali potrebbero essere unici quanto le organizzazioni che servono. È importante che l›organizzazione definisca il motivo per cui sta costruendo un CERT, quale sarà la sua missione e quali obiettivi vuole proporsi, per poter rispondere alle precedenti domande.

Il caso della Provincia Autonoma di Trento

Un esempio di questo approccio è rappresentato dal percorso seguito dalla Provincia Autonoma di Trento che sta approntando il **CERT-PAT**.

Nel 2011, l'in-house della Provincia Autonoma di Trento, Informatica Trentina, ha esternalizzato la gestione delle componenti di rete e sicurezza attivando un servizio di NOC/SOC, con l'obiettivo di potenziare e centralizzare la gestione della sicurezza.

Nella prima fase di attivazione e successivo consolidamento della struttura non è stato possibile separare nettamente il NOC - attività molto operativa legata alla gestione degli apparati che garantiscono il corretto funzionamento dell'infrastruttura, indipendentemente dal loro ruolo - dal SOC - attività di monitoraggio della sicurezza, di prevenzione e gestione degli incidenti di sicurezza, di indirizzo per soggetti terzi, e tra questi, il NOC – in quanto le aree di sovrapposizione, nell'organizzazione storica dell'azienda, non permettevano di distinguere nettamente i diversi ambiti.

Per questa ragione, la società ha deciso di procedere per gradi, sfruttando le competenze interne, traguardando l'obiettivo finale di avere i due servizi con ruoli e compiti definiti e distinti.

Nel 2017 il processo si è concluso, affidando la responsabilità del servizio SOC all'unità interna di Cybersecurity, mentre il NOC è rimasto di competenza della funzione Datacenter.

Con questa nuova organizzazione, il SOC ha stretto relazioni con il CERT Nazionale e il CERT-PA, e ai processi tipici di uno SOC si sono affiancati quelli tipici del CERT.

Nel frattempo, nel 2014, con lo scorporo del ramo di azienda della in-house che includeva anche la gestione della sicurezza della rete, confluito in Trentino Network, in-house deputata allo sviluppo e alla gestione della rete di telecomunicazioni provinciali, il NOC/SOC ha continuato ad erogare i propri servizi per entrambe le società, raccogliendo ed elaborando tutte le informazioni (log) generate dai sistemi informativi e dagli apparati di rete delle due organizzazione e allertando, di volta in volta, le strutture di riferimento con segnalazioni, apertura di incidenti di sicurezza e bollettini informativi.

L'attuale configurazione garantisce il monitoraggio di gran parte del traffico della rete provinciale, che resta comunque un ecosistema complesso all'interno del quale convivono numerose realtà, grandi e piccole, le cui attività possono avere ricadute, anche rilevanti, sull'intera infrastruttura. Su molte di queste il SOC ha una visibilità molto limitata, se non addirittura nulla.

Questa situazione porta principalmente a due conseguenze negative: da un lato, per gli eventi che vengono rilevati e che hanno origine/terminano nelle infrastrutture non monitorate, non è possibile stimare correttamente l'entità (anche potenziale) e le eventuali ripercussioni che potrebbero avere sui servizi erogati dall'ente provinciale; dall'altro, per gli eventi che si verificano all'interno di tali infrastrutture ed hanno impatto limitato al loro perimetro, non vi è la possibilità di nessuna azione reattiva, in quanto l'evento stesso resta sconosciuto.

Per affrontare questa problematica nel febbraio 2017 è stato creato un gruppo di lavoro dedicato al tema della Cyber Security e della Privacy, avente come principale obiettivo la progressiva costituzione di un SOC-CERT integrato tra gli Enti, come entità di coordinamento nell'ambito cybersecurity, entro la fine del 2017.

I lavori del gruppo hanno portato alla progettazione del servizio, il cui avvio è previsto nei primi mesi del 2018, che avrà un'organizzazione semplice e snella, a garanzia di una prontezza di reazioni in caso di emergenza.

L'organizzazione ipotizzata, prevede:

- **Comitato guida**: il CERT-PAT erogherà servizi per enti anche molto diversi tra loro, garantendo la massima efficienza nell'erogazione dei servizi. Per questa ragione, ogni ente membro della comunità di riferimento dovrà identificare il soggetto che farà parte del comitato. Ogni membro del comitato, per l'ente di riferimento, garantirà la disponibilità di proprio personale, se necessario, per la gestione di incidenti di sicurezza.
- **Coordinamento del CERT-PAT**: il coordinamento del CERT-PAT verrà affidato alla funzione Cybersecurity, già responsabile del SOC interno dell'azienda, che garantisce anche il monitoraggio dell'infrastruttura provinciale.

- **Strumenti di comunicazione**: verrà creato un sito web dedicato per annunciare le informazioni relative al CSIRT. Una mailing list verrà installata e mantenuta, con una parte riservata alla comunicazione tra i membri del gruppo e con altri gruppi. Tutti i dettagli dei contatti dei membri del personale sono archiviati in una banca dati e una stampa viene conservata nella cassaforte.
- **SOC/CERT-PAT**: è la componente operativa del CERT-PAT che eroga i servizi previsti. La dotazione tecnologica del CERT-PAT sarà un'infrastruttura dedicata esclusivamente a tale servizio, isolata dal resto dell'infrastruttura e gestita internamente, a garanzia di una corretta *segregation of duties*, senza ricorrere a personale delle altre funzioni.

Il caso della Regione Friuli Venezia Giulia

Un altro approccio utilizzato per l'istituzione di un CERT territoriale è costituito dal caso del CERT-RAFVG della Regione Autonoma Friuli-Venezia Giulia. Tale processo ha previsto una dinamica di tipo bottom-up, originata non tanto dalla volontà *ex ante* di definire una pletora di servizi CERT nell'ambito di un sistema che presenti una certa frammentazione, ma piuttosto: dalla definizione *ex ante* di un sistema integrato regionale che raccoglie gli Enti del territorio (Regione, Aziende Sanitarie ed Enti Locali); dalla previsione di servizi informatici omogenei e evoluti in maniera coordinata; dalla definizione di servizi di sicurezza ed estrazione e dalla caratterizzazione di tali servizi, già presenti nei fatti, che si inquadravano nel modello tassonomico definito per la costituzione di uno CSIRT.

Successivamente, grazie alla presa di coscienza circa il modello di erogazione dei servizi CERT, a partire dal 2005, essi sono potuti evolversi tenendo sempre in considerazione tale tassonomia.

Schematicamente le fasi seguite sono state:
- definizione di un sistema informativo integrato;
- definizione di standard e servizi in relazione alla sicurezza delle informazioni;
- inquadramento dei servizi erogati nella tassonomia definita per un CERT:
  - Servizi reattivi;
  - Servizi proattivi;
  - Servizi di *quality management*;
- evoluzione dei servizi di sicurezza, sempre tenendo conto della tassonomia definita.

Queste le caratteristiche primarie di questo tale di sviluppo:
- lo sforzo primario degli interventi connessi allo sviluppo del sistema si è potuto concentrare *in primis* non tanto sulla definizione di procedure

o regole di ingaggio e comunicazione tra gli attori del sistema regionale ed il CERT, quanto principalmente sulla definizione di modelli di servizio omogenei per la sicurezza delle informazioni, che essendo costruiti in maniera comune e gestiti attraverso l'in-house in maniera coordinata, potevano beneficiare di una regia coerente.

- partire dai servizi erogati ha consentito, soprattutto nell'erogazione della componente core dei servizi CERT (ovvero la risposta agli incidenti), di avere dei vantaggi operativi quali:
  - disponibilità di informazioni di prima mano derivanti direttamente dai servizi offerti, che non vengono fornite al CERT da una terza parte e hanno un livello di verificabilità e attendibilità mediamente più elevato;
  - possibilità di intervenire direttamente, senza intermediazione, sui servizi di erogazione per mitigare gli effetti di un attacco informatico;
  - avere una "massa critica" sufficiente a disporre di personale dedicato alla sicurezza delle informazioni;
  - specializzare le risorse dedicate alla sicurezza delle informazioni in relazione alle peculiarità dei servizi offerti alla Constituency;
  - mettere a disposizione conoscenze specifiche sulla sicurezza delle informazioni a tutti gli attori del sistema regionale (in-house, Enti) in maniera puntuale e tarata sul contesto specifico;
  - poter rappresentare a livello degli organismi nazionali ed internazionali le esigenze derivanti dalla peculiarità del territorio;
- nonostante la sussistenza di tali vantaggi, è oggi attuale la necessità di definire dei modelli di comunicazione efficaci e concordati per l'interazione con omologhe realtà extra regionali, tenendo conto della necessità di non stravolgere le modalità operative in essere.

Anche volendo seguire un approccio di questo tipo, gli interrogativi da porsi sono molto simili a quelli indicati in precedenza.

Piattaforme di base per la costruzione di un CERT

Il monitoraggio efficace degli incidenti dovrebbe seguire un processo ben definito ed univoco, che coinvolga personale appropriato e acquisisca determinati dati durante ciascun caso. Il CERT Territoriale dovrebbe considerare come i dati dei singoli incidenti potrebbero essere collegati in modo che i modelli e le tipologie dei dati possano contribuire sia a rendere più efficace la missione di risposta agli incidenti sia a migliorare il livello preventivo di sicurezza sul territorio di competenza.

Per raggiungere questo obiettivo è fondamentale concentrarsi sulle capacità fondamentali che un CERT dovrebbe esprimere rispetto alla tassonomia del

Cybersecurity Framework (in ordine: *Prepare, Detect, Analyse, Respond, Recover*):

- **ricezione, analisi, ed archiviazione delle informazioni degli incidenti**: oltre alle informazioni presenti nelle banche dati delle vulnerabilità (Mitre Common Vulnerabilities and Exposures, NIST National Vulnerability Database ed Exploit-db, per esempio – il FIRST mantiene una lista aggiornata: **https://www.first.org/global/sigs/vrdx/vdb-catalog**) e agli aggiornamenti costanti ricevuti da bollettini e allerte distribuite dalla rete dei CERT nazionali, europei e di infrastruttura (cosiddetti *verticali*), il CERT dell'organizzazione deve anche essere il punto di accentramento di tutti i rapporti di violazione della sicurezza cibernetica o dei dati di terzi, in modo da essere punto di contatto e di interazione unico dal punto di vista legislativo – che si parli di NIS, GDPR o legislazioni nazionali o di settore – e mantenere contatto e supporto nei confronti degli attori coinvolti.
- **conoscenza granulare, profonda e in *realtime* della configurazione della rete e degli *asset* presenti**: una *consolidated cyberspace picture* è alla base della superiorità conoscitiva dell'ambiente operativo. In questo caso il teatro in cui si svolgono le operazioni è il segmento di *cyberspace* che riguarda la rete supervisionata dal CERT, che di conseguenza deve avere a disposizione tutte le informazioni che agenti, sonde, firewall e più in generale sensori sono in grado di recepire e trasmettere. Questa capacità è realizzata nel SIEM, come già citato in precedenza, che quindi diventa il cuore della capacità di raccolta e prima analisi della situazione. Esistono SIEM open source o gratuiti, tuttavia il valore mancante in queste soluzioni è la grande quantità di interrogazioni, schermate e cruscotti (*query, screens* e *dashboards*) predefiniti e *industry-grade*, tali da ridurre il tempo di messa in opera del sistema – posto anche che ogni rete ha le sue specificità, quindi c'è sempre un secondo livello di raffinamento dello strumento una volta integrato nel complesso della sicurezza. Fa parte di questa capacità anche l'identificazione e la gestione degli eventi e del flusso di risposta (*workflow*). Il servizio di *ticketing* è quindi fondamentale nella individuazione e nella successiva gestione della risposta, potendo tracciare, sia nel tempo che nel contenuto, tutti gli eventi che possono portare ad un incidente o ad una breccia. Grazie a questa visione olistica degli eventi diventa una risorsa importante quando è necessario andare a risalire agli indicatori di compromissione o durante le fasi di *response* e *recovery* da un incidente di sicurezza cibernetica. Tutta questa mole di informazioni viene poi conservata per futura fruizione, con l'opportuno *need to know*. Una delle piattaforme open source più famose nel *ticketing* e come *task tracker* è RTIR.
- **analisi e gestione continua del rischio cibernetico**: la superiorità conoscitiva raggiunta tramite una sapiente disposizione (*deployment*) dei sensori nella rete di competenza è soltanto il primo fattore abilitante per una

full operational capability. Tramite questo grande volume di dati è possibile estrarre informazione a supporto della decisione dell'assetto del CERT, stimando continuativamente e persistentemente il livello di rischio cibernetico in modo dinamico, partendo dagli eventi nella rete e combinandoli con il framework di governo e gestione in atto nell'organizzazione. In particolare potrebbe accadere che con un rischio basso si potrebbe delegare interamente il livello di attenzione al SOC, con un rischio medio avere in azione la struttura del CERT e con un rischio alto valutare una escalation alla presenza di un rappresentante della struttura della gestione delle crisi. In questo ambito sono di grande utilità gli strumenti messi a disposizione da consessi di attori aventi causa in questo panorama, come ad esempio l'ISF (Information Security Forum), che condivide con i suoi partecipanti il database e la metodologia IRAM2, che copre rischi e vulnerabilità in modo continuamente aggiornato.

- **analisi e gestione delle vulnerabilità**: un'altra capacità fondante di un CERT è la possibilità di eseguire *vulnerability assessment* e *vulnerability management*. Queste funzioni impongono da un lato requisiti non soltanto di dotazione software, ma strutturali riguardo l'architettura fisica del CERT. Gli impatti architetturali per poter compiere analisi di una minaccia potenziale o confermata e non ancora identificata possono essere meglio visualizzati con un parallelo biologico nel caso di agenti patogeni per l'uomo gravissimi, letali o addirittura sconosciuti (o per cui è sconosciuta una cura) – cosiddetti *Biohazard Level 4*. Nel manipolare agenti a rischio così elevato – che sono l'equivalente biologico delle *cyberweapons* e delle *weaponised vulnerabilities* – è obbligatorio l'uso di una tuta a pressione positiva insieme ad una riserva d'aria segregata. Nel parallelo cibernetico, questo implica essere consci che, data la costante e polimorfica evoluzione dei *malware* e delle armi cibernetiche, dovremo essere pronti a misure di estrema segregazione personale nel lavorare con questi *patogeni cibernetici*, simili e anche più estese di quelle necessarie nelle sale TEMPEST. Un laboratorio che gestisce patogeni *Biohazard Level 4* ha ingressi ed uscite con docce multiple, una camera a vuoto, una camera ultravioletta, sistemi di individuazione autonomi ed altre precauzioni di sicurezza progettate per distruggere tutte le tracce del patogeno. *Airlock* multipli impediscono l'apertura delle porte contemporaneamente – e tutta l'aria e l'acqua di servizio che vengono immesse o prese da un laboratorio di questo livello subiscono lo stesso trattamento per eliminare la possibilità di una contaminazione accidentale. Nel parallelo cibernetico dobbiamo impiegare gabbie di Faraday per impedire comunicazione elettromagnetica tra più dispositivi all'interno del laboratorio, reti fisicamente separate e su infrastrutture segregate (*multi-layered air-gapping*), raddoppio e ridondanza delle misure di protezione *outward-facing* e modulari interne, uso di tecniche di intelligenza artificiale per *anomaly detection* e risposta automatica – quando non autonoma. Il tutto da aggiungere agli

adempimenti legali per mantenere integra la *chain of custody* nel caso in cui il CERT si occupi anche di *forensics* (per esempio armadi corazzati o casseforti, in grado di resistere a fuoco diretto ed incendi).

- **Condivisione delle informazioni**: il cuore su cui si fonda una corretta operatività del CERT. Questo processo permette agli *stakeholder* lo scambio di informazioni delicate e privilegiate mantenendo la confidenzialità e la fiducia nella comunicazione e mantenendo la sicurezza delle informazioni. Per essere univoci ed avere una base comune in questo processo spesso si utilizza un codice-colore abbinato alle informazioni di incidente, chiamato Traffic Light Protocol (TLP), che prevede un insieme di requisiti per far sì che ogni informazione condivisa sia distribuita solo ai destinatari corretti. Il TLP prevede 4 colori (di solito White, Green, Amber e Red in ordine di crescente gravità) ad indicare le prescrizioni di confidenzialità e condivisibilità dell'informazione di incidente che i riceventi dovranno adottare nel gestirla. Questo solitamente si traduce nei *"5 Right"*: *Right information, at the right time, in the right place, displayed in the right format to the right person*.
- Tutto questo supportato e validato da una solida **capacità di intelligence** in tutti i livelli del web e del tessuto del *cyberspace*, in grado di convogliare, analizzare, valutare e valorizzare il volume, la velocità e la varietà dei *big data* che si riversano in ogni secondo nello spazio cibernetico ed ottenere delle risposte in tempo quasi reale o proattive (per esempio la *identity protection*).

Principi di base sull'autonomia, l'isolamento e la resilienza dell'infrastruttura a supporto del CERT

L'errore più grande che fanno molti CERT di nuova costituzione è quello di sottovalutare la gestione delle proprie infrastrutture e dei propri strumenti base ICT. L'utilizzo di software open source (es. RTIR, il software più utilizzato) è molto spesso non accompagnato dalla necessaria attenzione alla resilienza della propria infrastruttura ICT (posta elettronica, server aziendali, linee di accesso a internet aziendali, ecc.), con la conseguenza che questi sistemi sono proprio le prime tessere del domino a cadere durante un attacco. I CERT dovrebbero essere dotati di un'infrastruttura dedicata, indipendente e possibilmente sviluppata con una logica diversa rispetto a quella aziendale.

La visione architetturale – riferendosi con questo solo all'infrastruttura tecnologica e non di governo o di *policy* – per la creazione di un CERT deve necessariamente indirizzare gli aspetti interni necessari all'erogazione dei servizi, in primis, e solo dopo un catalogo di servizi CERT. Questa visione può essere articolata in tre aree: sicurezza fisica, *storage*, e infrastruttura di rete.

La *sicurezza fisica* degli ambienti del CERT deve essere progettata in modo tale da garantire dei livelli appropriati di privacy e protezione delle informazioni del CERT e delle sue aree. Alcuni aspetti più immediati da considerare sono la disponibilità di aree dedicate per ogni rappresentanza all'interno del CERT, aree sicure per tutti i server e le *repository* di dati del CERT, così come casseforti o armadi corazzati per le informazioni e i dati non elettronici. Altri, forse meno ovvi, sono la disponibilità di linee cifrate e sicure di comunicazione interna ed esterna –telefoni, fax, email, schemi crittografici oppure la separazione degli operatori in servizio dal resto dell'organizzazione (controllo accessi, isolamento acustico e visivo, sale riservate agli eventi di crisi). La separazione e segregazione è anche un principio guida dell'ambito dello *storage*, che deve essere eseguito sulla base della classifica dell'informazione gestita e dello scopo per cui si immagazzina. La posizione dell'area di storage e al suo interno il modo di allocare il materiale conservato sono temi da considerare in fase di progetto; ad esempio, come sono disposti materiali di classifica diversa? In che modo è segmentato l'accesso? Come sono divisi materiali con sensibilità forense dagli altri? Una risposta pronta a queste domande indica una adeguata considerazione dell'infrastruttura prima della missione. In ultimo, l'infrastruttura su cui maggiormente il CERT opera, quella di *rete*. Per iniziare, un CERT non può prescindere dall'avere una *test network* fisicamente separata da ogni altra rete presente e che abbia un accesso ad internet proprio e non condiviso. Per la *operative network* ci deve essere piena visibilità, responsabilità e presa in carico dell'infrastruttura (p. es. DNS, e-mail, web servers, computers, backup), utilizzo di comunicazioni sicure ed anche PGP per *cryptographic privacy* ed autenticazione. In ultimo avere anche una CERT LAN, ancorché fisicamente separata da ogni altra rete presente, permette una modalità più spedita di operazioni e condivisione – ma con maggiore connettività arriva anche maggiore necessità di essere vigili.

I cyber exercise come elemento abilitante per rafforzare le capacità di risposta agli incidenti dei CERT

I team di risposta agli incidenti dei CERT sono chiamati a coordinare la risposta agli incidenti con il coinvolgimento di molteplici stakeholder - interni ed esterni alle organizzazioni - inclusi i vertici aziendali nei casi di particolare criticità. Questi ultimi necessitano tuttavia di una chiara comprensione di impatti, effetti e modalità di gestione degli incidenti, per esercitare consapevolmente la loro responsabilità in termini di gestione del rischio. Analogamente è essenziale e ragionevole verificare le capacità di risposta agli incidenti delle organizzazioni - sia in termini di processi che di controlli, procedurali e tecnici, implementati per proteggere gli asset.

Per facilitare questo processo di sensibilizzazione del personale ed in particolare dei vertici aziendali da un lato e dall'altro permettere di valutare l'efficacia della risposta agli incidenti del personale operativo sono sempre più impiegate tecniche così dette di *cyber exercise*.

I *cyber exercise* sono attività che prevedono, tramite una serie di esercitazioni, di coinvolgere i partecipanti in uno scenario interattivo nel quale vengono simulati uno o più attacchi informatici. I partecipanti sono chiamati a gestire i differenti scenari con l'obiettivo di evidenziare possibili aree di miglioramento che le tecniche di difesa devono colmare al fine di raggiungere un livello di maturità ottimale e di esercitare le capacità in modo che sia possibile reagire tempestivamente al verificarsi di un incidente, garantendo un'efficace coordinazione tra le diverse funzioni.

Gli scenari sono definiti solitamente da specialisti con elevate competenze di Cyber Security e Cyber Intelligence, capaci di mutuare tattiche e metodologie del mondo militare ed accademico, in un contesto simulato che permetta di comprendere quali effetti comporterebbero eventuali incidenti, e quali siano i processi da definire o migliorare per fronteggiarli in modo sicuro a tutela dell'organizzazione stessa. Gli scenari possono coinvolgere diversi partecipanti, fra i quali: vertici aziendali, manager, rappresentanti di specifiche funzioni o uffici, personale tecnico specializzato in materia di Incident Response, fornitori esterni, ecc.

Tipicamente un servizio di cyber exercise prevede diverse possibili modalità di erogazione:

- **Cyber Drill** I partecipanti vengono guidati attraverso la risposta pianificata dell'organizzazione alla risoluzione di un incidente cyber. Sono informati inoltre sulle loro specifiche responsabilità e ruoli nell'area dei rischi cyber e nelle strutture di sicurezza così come il rispettivo contesto legale.
- **Cyber Table Top** I partecipanti valutano direttamente e con limitato supporto le loro capacità di rispondere a un incidente cyber mediante l'uso di uno scenario simulato. Gli sviluppi vengono pianificati in anticipo ed includono una sequenza predefinita di contributi.
- **Cyber Wargaming** I partecipanti testano le proprie abilità per poter rispondere ad un cyber incident in evoluzione e dinamico – l'evoluzione dello scenario è basato su azioni e decisioni del partecipante. Solitamente sono coinvolti diversi stakeholders su diverse sedi mediante piattaforme e tool di simulazione.

SEZIONE 2: *INFORMATION SHARING*

a cura di **Stefano Plantemoli** (Ministero dell'Interno) e **Giovanni Mellini** (ENAV)

Definizione di cyber threat Intelligence e Introduzione all'infosharing

Da sempre il compito degli analisti di sicurezza è studiare, analizzare e comprendere il comportamento dell'attaccante. Nella protezione dei nostri patrimoni informativi la capacità di capire il modo in cui chi ci minaccia pensa e opera, la comprensione delle sue motivazioni e l'identificazione delle tattiche utilizzate ci consente di prendere decisioni, implementando così possibili azioni di rimedio. Indipendentemente dall'attore o dallo scenario che origina un evento cyber, le operazioni di intelligence guidano entrambe le parti. La parte che meglio riesce a interpretare l'intelligence, analizzando le informazioni sullo scopo, la capacità e le opportunità degli avversari, sarà quasi sempre in posizione di vantaggio.

In questi ultimi anni, la minaccia cyber è in continua espansione dato che gli strumenti e le tattiche di attacco sono sempre più numerose, e le loro motivazioni vanno dalla raccolta di credenziali e password, al guadagno finanziario, alla distruzione dei servizi fino alla distorsione delle informazioni. Comprendere chi ci minaccia è diventato molto più complicato, poiché che ciò deve essere compiuto in tempi più brevi rispetto al passato.

L'aspetto che può ridurre i tempi nella comprensione di chi fronteggiamo è l'introduzione dell'intelligence nei processi di risposta degli incidenti ed indubbiamente la condivisione delle informazioni a nostra conoscenza durante le varie fasi della gestione dell'incidente informatico. La *Threat Intelligence* (TI) è l'analisi degli avversari: le loro capacità, motivazioni e obiettivi, mentre la *Cyber Threat Intelligence* (CTI) è l'analisi di come gli avversari utilizzano il dominio cibernetico per raggiungere i loro obiettivi.

Le informazioni dovrebbero essere analizzate e le loro implicazioni comprese per applicare le opportune azioni di prevenzione, con lo scopo di individua-

re e sradicare al meglio le minacce. **Le azioni intraprese per comprendere meglio gli avversari dovrebbero diventare un processo formale come parte critica delle operazioni di sicurezza delle informazioni**.

L'intelligence è spesso definita come l'informazione che è stata raffinata e analizzata al fine di renderla utilizzabile. La TI richiede quindi informazioni. Nella gestione degli incidenti basati su questo approccio esistono diverse modalità per raccogliere informazioni che verranno analizzate, correlate e utilizzate per supportare al meglio la risposta agli incidenti informatici. È importante notare che la risposta agli incidenti genererà a sua volta ulteriore intelligence sulla minaccia osservata, dando vita ad un *"ciclo di cyber intelligence"* in termini di direzione, raccolta, elaborazione, analisi, diffusione e relativo feedback. La risposta agli incidenti basata sull'intelligence aiuta a migliorare le politiche di sicurezza e supporta anche una formazione mirata per la consapevolezza degli utenti. La risposta agli incidenti così strutturata non termina quando l'intrusione viene compresa e risolta, **ma realtà genera informazioni che continueranno ad alimentare il ciclo di intelligence.**

L'analisi di un'intrusione, riuscita o fallita, può fornire una varietà di informazioni che possono essere utilizzate per comprendere meglio la minaccia globale per una struttura. La causa principale dell'intrusione e il vettore di accesso iniziale possono essere analizzati per informare un'organizzazione dei punti deboli nelle proprie difese di rete o delle politiche di cui gli attaccanti potrebbero abusare. Il malware identificato su un sistema può aiutare a identificare le tattiche che gli aggressori stanno usando per eludere le misure di sicurezza poste in essere.

La condivisione di queste informazioni con altre strutture consente di aumentare la capacità reattiva di tutti, abilitando una fase di maggiore maturità dei partecipanti nel processo di infosharing e un arricchimento dell'informazione originaria per consentire valutazioni più precise.

I problemi tipici con cui l'analista si confronta includono:

- Quale ISP gestisce questo indirizzo IP?
- La connessione a questo indirizzo IP è corretta?
- A quale Autonomus system appartiene?
- Questa URL è pericolosa?
- Chi ha registrato il dominio?
- Quali tipi di minacce sono state fornite su questo sito?
- Questa URL è collegata ad altra attività dannosa?
- Quali vulnerabilità presenti nel mio ambiente vengono attivamente sfruttate su Internet?
- Chi sono gli attori delle minacce che vendono o utilizzano queste vulnerabilità?

Questi gli aspetti più importanti della condivisione delle informazioni:

- L'intero concetto di condivisione delle informazioni è basato sulla **fiducia**. Questa può esistere a livello personale, con un individuo che si fida di un altro, o può esistere tra gruppi di persone all'interno di organizzazioni diverse che condividono un interesse comune sul tema.
- Le informazioni da condividere richiedono una qualche forma di **classificazione delle informazioni**. Molte iniziative di condivisione delle informazioni ora fanno uso del ***Traffic Light Protocol*** **(TLP)** per stabilire il modo in cui le informazioni da condividere devono essere gestite.
- Le informazioni devono essere **accurate**. È inutile condividere informazioni che non sono state verificate.
- La comunicazione agli altri deve essere **tempestiva**. Questo può impedire ad un utente malintenzionato di avere una finestra temporale lunga per avviare o replicare un attacco che sfrutta metodologie o vulnerabilità nuove.
- La condivisione deve essere **eseguita con cura**. La cerchia delle parti interessate con le quali le informazioni sono condivise deve essere considerata attendibile per gestirle in un modo concordato e non per permettere che venga diffusa diversamente. Dovrebbero esserci meccanismi integrati nel processo per impedire la distribuzione a persone o organizzazioni esterne al gruppo di condivisione.
- Dovrebbe essere possibile **anonimizzare la fonte delle informazioni**. Occasionalmente, rivelare l'identità dell'organizzazione che ha sollevato il problema potrebbe rivelarsi dannoso, pertanto un mezzo per trasmettere le informazioni senza attribuzione è essenziale.

Utilizzo della Threat Intelligence

L'utilizzo della CTI deve rappresentare un'occasione per migliorare le proprie capacità di gestione degli incidenti informatici, agendo in maniera più rapida ed efficace e migliorando le fasi di preparazione, *triage* e contenimento. Ad oggi le informazioni di IoC spesso vengono ricevute in maniera non strutturata, non contestualizzata, da canali diversi ed in alcuni casi in maniera duplicata, ciò non consente l'automazione necessaria ed utile a diminuire il caricamento e la relativa correlazione di quanto ricevuto. Va compreso che, indipendentemente dal livello di maturità della struttura che le riceve, vi sono una serie di aspetti che andrebbero sempre tenuti in considerazione, quali: l'aggiornamento dell'informazione (*versioning*), il contesto della informazione, l'arricchimento della stessa.

Quando si parla dell'aggiornamento dell'informazione si intende indicare la validità della stessa al momento della ricezione. Ad esempio, ricevere un'informazione su un indirizzo IP di C&C non più attivo porta ad un'inibizione forse inutile del traffico, viceversa ricevere ulteriori domini malevoli su un medesimo IP contribuisce ad aumentare le capacità di prevenzione di un determinato malware.

Il contesto dell'informazione è uno degli aspetti più importanti. Troppo spesso veniamo in possesso di informazioni riguardanti campagne attive in ambienti operativi non di nostra competenza, quali ad esempio attacchi su reti SCADA ricevuti da ambienti bancari o finanziari. Risulta evidente la perdita di tempo in questo scenario, ma spesso si commette un errore ancora più grave scartando degli eventi che accadono sulle nostre reti perché ritenuti non significativi o pericolosi per i nostri domini di competenza, senza darne conto ad un CSIRT che potrebbe invece trovarli utili.

Un ultimo aspetto è rappresentato dall'arricchimento del dato. In alcuni scenari può essere molto utile conoscere l'*autonomous system* di alcune reti o indirizzi IP, l'attore che conduce una determinata campagna, le metodologie utilizzate e i vettori d'attacco.

Il primo naturale utilizzo delle informazioni di Threat intelligence è quello della prevenzione, ma è riduttivo usare questo tipo di informazioni solo per attività tipiche di un SOC, bisogna realizzare uno scambio informativo strutturato e controllato che alimenti non solo il SIEM e gli strumenti di prevenzione, ma se possibile anche una piattaforma di Threat Intelligence che inizi a mostrare relazioni tra diverse campagne e le metodologie utilizzate, tutto a vantaggio del processo di gestione dell'incidente sia in termini di riduzione dei tempi che di chiarezza dello scenario che ci si trova a fronteggiare.

La ricezione di informazioni di intelligence in forma non strutturata, seppure non direttamente utilizzabili nello strumento, aumentano sicuramente le conoscenze e la sensibilità dell'analista di sicurezza, che può venire a conoscenza di nuove tecniche di attacco e del loro utilizzo in campo. Se tutta questa informazione, in aggiunta a ciò che viene raccolto ed analizzato dai sistemi posti sotto la propria gestione, fosse disponibile in maniera strutturata, si compirebbe un enorme passo avanti per la prevenzione e il contenimento delle campagne malware.

Definizione di STIX

L'obiettivo di **STIX** (*Structured Threat Information eXpression*) è quello di specificare, caratterizzare e acquisire le informazioni sulle minacce informatiche. STIX affronta una gamma completa di casi d'uso delle minacce informatiche, tra cui analisi delle minacce, acquisizione e specifica degli indicatori, gestione delle attività di risposta e condivisione delle informazioni, per migliorare la coerenza, l'efficienza, l'interoperabilità e la consapevolezza generale della situazione.

STIX è un modello di dati grafico basato su *edge* e *node*. I nodi sono *STIX Data Objects* (SDO), mentre gli edge sono *STIX Relationship Objects* (SRO). Gli SDO in-

cludono informazioni come Metodi di attacco, Identità, Dati osservati, Threat actor, Vulnerabilità, ecc.

Gli SRO (edge) sono pensati per connettere gli SDO in modo che, nel tempo, gli utenti saranno in grado di sviluppare una conoscenza approfondita degli attori delle minacce e delle loro tecniche.

Il formato STIX 2.0 definisce 12 STIX domain Objects (SDOs). Tra i più utili alla fase di prevenzione troviamo:

- **Observables**: rappresenta informazioni sulle proprietà *stateful* o eventi misurabili inerenti il funzionamento di computer e/o reti. Informazioni su un file (nome, hash, dimensione, ecc.), un valore di chiave del Registro di sistema, un servizio avviato o una richiesta HTTP inviata sono tutti esempi di observables;
- **Indicators**: Contiene un modello che può essere utilizzato per individuare attività cyber malevole o sospette. I valori qui contenuti possono essere hash di file oppure URL. Mette in relazione questi pattern osservabili a particolari TTP che i *threat actors* impiegano. **Gli indicatori sono le informazioni più comuni fornite oggi nella Threat Intelligence**;
- **TTP**: termine preso in prestito dall'ambito militare "**Tattiche, tecniche, procedure**" per rappresentare il comportamento o il modus operandi dell'avversario quando esegue l'attacco. Un TTP può contenere informazioni su quali siano le vittime del *threat actor*, quali modelli di attacco e malware vengono utilizzati, e quali risorse (infrastrutture, strumenti, persone) vengono sfruttate;
- **Exploit Targets**: contiene informazioni su una vulnerabilità tecnica, debolezza o errata configurazione nel software, sistemi o reti che potrebbero essere oggetto di uno sfruttamento da parte di un *threat actor*.

Questi elementi STIX possono sicuramente fornire, una volta ricevuti, un contributo notevole alimentando i SIEM di una organizzazione per ottimizzare gli allarmi e le regole di correlazione. Si tenga presente che oggi sono già numerose le piattaforme di prevenzione e di analisi log ed eventi in grado di importare in maniera nativa questo formato.

Come indicato in precedenza, vi sono però altri SDO che possono certamente aiutare il lavoro dell'analista e dare maggiori informazione alle piattaforme di intelligence favorendo quello che possiamo chiamare l'arricchimento del dato:

- **Campaign:** rappresenta un insieme di attività e comportamenti che gli attori della minaccia eseguono per ottenere l'effetto desiderato in un periodo di tempo.
- **Course of Action**: rappresenta una serie di attività che possono essere prese in risposta ad un attacco o come misura preventiva allo stesso.

- **Threat Actor**: caratterizza o identifica l'attaccante o l'avversario. Fornisce informazioni quali l'identificazione delle caratteristiche, la sofisticazione del *threat actor*, le sue motivazioni e il comportamento osservato in passato.

Risultano evidenti, anche in questa brevissima introduzione dello STIX, le potenzialità del framework e le opportunità che lo scambio di queste informazioni possa portare alle varie organizzazioni partecipanti.

In campagne Cyber di rapida diffusione la possibilità di rendere disponibili gli Ioc e gli Observables in tempo quasi reale consentirebbe una pronta azione di rimedio a chi produce e consuma queste informazioni in maniera automatizzata, i CSIRT potrebbero veicolare informazioni arricchite anche ad organizzazioni non opportunamente preparate da un punto di vista della Cyber security.

Definizione di TAXII

Nato per soddisfare le esigenze di condivisione delle informazioni tra diversi settori di infrastrutture critiche, questo protocollo consente e assicura il passaggio delle informazioni in modo controllato. ***Trusted Automated eXchange of Intelligence Information*** **(TAXII)** è un protocollo applicativo per lo scambio di Cyber Threath Intelligence su HTTPS. TAXII definisce una RESTful API (un insieme di servizi e scambi di messaggi) e una serie di requisiti per TAXII Client e Server.

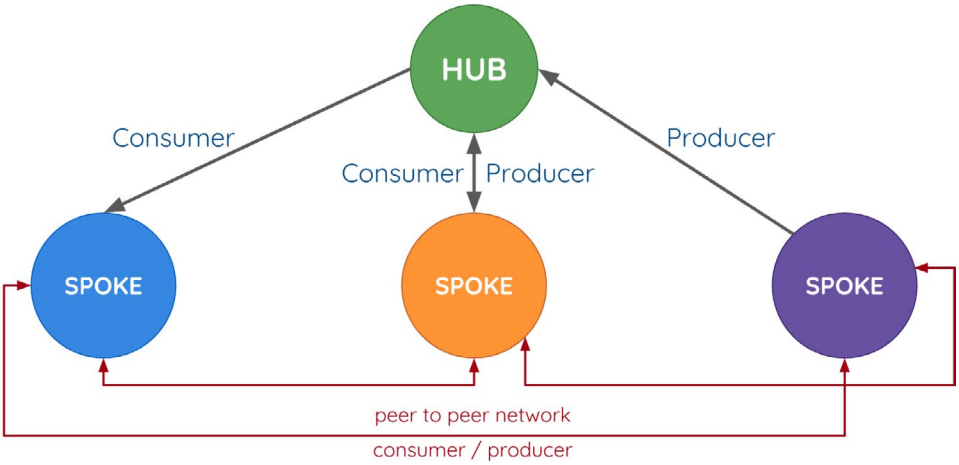
TAXII definisce un insieme di servizi e scambi di messaggi che, una volta implementati, consentono la condivisione di informazioni sulle minacce informatiche utilizzabili attraverso i confini dell'organizzazione e dei prodotti / servizi per l'individuazione, la prevenzione e la mitigazione delle minacce informatiche.

Architettura e modello dati

Considerata la scelta del linguaggio STIX per la definizione delle minacce CTI (*Cyber Threat Intelligence*) ed il protocollo TAXII come meccanismo di trasporto per la condivisione delle stesse tra enti/organizzazioni differenti, l'obiettivo è quello di creare una rete efficace ed efficiente (community) in cui il semplice indicatore scambiato (IP, URL, SHA, etc.) diventi, dopo la sua qualificazione, un'informazione.

Questo significa che gli indicatori, per poter essere trasformati in informazioni, devono essere rilevanti per tutta la community, che poi li utilizzerà in modi e per scopi differenti.

Modello di cooperazione CTI



Il modello di riferimento e cooperazione può essere sintetizzato in una architettura del tipo *hub&spoke* che prevede i ruoli di *producer* (colui che inietta le informazioni sulla rete) e *consumer* (colui che prende le informazioni dalla rete e le utilizza).

Modello di cooperazione CTI

Tale modello prevede un **HUB centrale (CERT)** deputato alla distribuzione degli indicatori ricevuti dai *producer* verso i nodi *consumer*, al fine di garantire un livello di protezione comune alla rete. Questo modello non preclude altresì la possibilità di attivare relazioni peer-to-peer tra elementi della community.

La maturità di una community è proporzionale al livello di capacità di utilizzo degli indicatori trasmessi, ovvero dalla capacità di trasformare questi indicatori in informazioni da poter utilizzare in contesti operativi di presidio quali i *Security Operation Center* (SOC) o strutture simili deputate al monitoraggio e alla risposta nel caso di incidenti informatici. È essenziale definire, vista la flessibilità del linguaggio STIX, una tassonomia minima di base che consenta a tutta la community di traguardare l'obiettivo di trasformare l'indicatore in informazione nei presidi operativi di sicurezza.

Segue un esempio pratico di tassonomia che include informazioni essenziali (principio del *need to know*) per poter descrivere una minaccia (WANNASHARE).

<stix:STIX_Header>
<stix:Title>**WANNASHARE**</stix:Title>
<stix:Description>**Threat: WANNASHARE**</stix:Description>
<stix:Short_Description>**YYYY-MM-DD HH:MM:SS**</stix:Short_Description>

Utilizzando questa semplice tassonomia è possibile tracciare in maniera efficace una minaccia nelle varie fasi della sua evoluzione

WANNASHARE	YYYY-MM-D1 HH:MM:SS	IoC1,IoC2
WANNASHARE	YYYY-MM-D2 H1:M1:S1	IoC3
WANNASHARE	YYYY-MM-D2 H2:M2:S2	IoC4,IoC5

Tutto ciò consente alle strutture operative di:

- includere gli indicatori nei sistemi di analisi in maniera automatica, consentendo una repentina reazione a seguito di match e la possibilità di esportare tali informazioni verso sistemi di protezione (es. firewall);
- utilizzare il tempo non investito in attività manuali di import ed analisi ad altre attività a più valore aggiunto.

Classificazione delle informazioni

Le informazioni da condividere devono essere classificate in base alla loro sensibilità e, qualunque sia il metodo utilizzato, dovrebbe poter essere utilizzato da entrambi i settori pubblico e privato senza la necessità di rimandi ai loro schemi di classificazione delle informazioni. Come indicato in precedenza, Il **protocollo TLP** viene utilizzato in molti processi di condivisione delle informazioni e classifica le stesse come uno dei quattro colori:

- **RED** - *Personale* - riservata ai destinatari specificati, la condivisione all'esterno del gruppo non è legittimata - nel contesto di una riunione faccia a faccia, ad esempio, la distribuzione delle informazioni RED è limitata a i presenti alla riunione.
- **AMBER** - *Distribuzione limitata* - i destinatari possono condividere questo tipo di informazioni con altri all'interno della propria organizzazione per finalità operative. Ci si può aspettare che il mittente specifichi i limiti previsti di tale condivisione.
- **GREEN** - *A livello comunitario* - le informazioni in questa categoria possono essere ampiamente diffuse all'interno di una particolare comunità o organizzazione. Tuttavia, le informazioni potrebbero non essere pubblicate su Internet, né rilasciate al di fuori della comunità.
- **WHITE** - *Illimitato* - le informazioni "bianche" possono essere distribuite liberamente e senza restrizioni in accordo con i termini di legge.

Questo metodo di classificazione delle informazioni è ampiamente utilizzato poiché è molto semplice da comprendere e implementare, e può essere facilmente comprese anche in altri settori o in Paesi stranieri. Nella maggior parte dei casi, il mittente delle informazioni da condividere determinerà il suo colore di classificazione, ma talvolta i CSIRT possono decidere di elevarlo se ritengono che il livello impostato sia troppo basso.

Il problema dell'anonimizzazione della sorgente di informazione si presenta, inevitabilmente, quando un'organizzazione partecipante non desidera essere identificata come vittima di un attacco (magari andato a buon fine) o come coinvolta in altro evento di sicurezza. Qualora l'organizzazione desideri che i dettagli dell'exploit siano resi disponibili alla comunità il CSIRT, si impegna a garantire che questa richiesta di anonimato sia rispettata, assicurando che, anche omettendo l'identità dell'originatore, le informazioni trasmesse non contengano indizi o metadati aggiuntivi che potrebbero in alcun modo rivelare, portare a dedurre, suggerire o identificare l'originatore.

SEZIONE 3:
CASI DI STUDIO

CERT: L'ESPERIENZA DI SOGEI

a cura di **Fabio Lazzini**, Sogei

Sogei in qualità di partner tecnologico del Ministro dell'Economia e delle Finanze e gestore di dati e infrastrutture critiche, ha sempre posto la massima attenzione agli aspetti di sicurezza ideando e realizzando strutture per il monitoraggio e la gestione della sicurezza stessa. Tale esperienza si è concretizzata con la realizzazione del CERT Sogei e con il continuo potenziamento e ampliamento delle risorse, sia umane che tecnologiche.

Le principali direttrici che hanno guidato la costituzione e l'evoluzione del CERT sono le best practice e le normative nazionali e internazionali quali la Direttiva NIS, il Piano Triennale per l'informatica nella PA e i diversi tavoli di confronto istituiti per stabilire una metodologia di scambio di informazioni e di indicatori relativi alla sicurezza IT. Negli ultimi mesi il CERT Sogei è stato, inoltre, coinvolto nelle attività di adeguamento al GDPR, in particolare nell'evoluzione dei processi, dei flussi e delle procedure riguardanti la gestione del "Data Breach".

Nel triennio 2015-2018 il CERT Sogei ha proseguito il suo lavoro focalizzando i propri sforzi su tre attività prioritarie quali il rafforzamento del ruolo di riferimento per le problematiche cyber per la propria constituency (sia interna che esterna), lo sviluppo di programmi di cyber security awareness, il potenziamento delle capacità di infosharing, orientate alla difesa preventiva dalla minaccia cyber.

I risultati particolarmente rilevanti riguardano la prima attività, in quanto si è registrato un significativo incremento del numero degli eventi gestiti, identificabili come "segnalazioni", "bollettini", "attività preventive" o "minacce reali" e "incidenti in corso".

Si è passati dai 347 eventi gestiti nel 2015 ai 1564 nel 2017.

Tale incremento è attribuibile alla maggiore capacità di analisi del CERT Sogei e a un sempre crescente flusso di segnalazioni provenienti dagli utenti, dipendenti Sogei e Clienti Istituzionali, segno tangibile del riconoscimento del CERT Sogei come principale struttura a cui rivolgersi per segnalare una possibile anomalia o un dubbio.

Le segnalazioni di un utente attento a tematiche di cyber security sono un elemento cardine del CERT. Da esse possono emergere incidenti di rilevanza critica; un esempio è il caso del malware "EyePyramid" che fu scoperto proprio grazie all'identificazione di una mail anomala da parte di una figura apicale di una delle società colpite dall'attacco.

L'analisi dei codici malevoli è una delle principali attività che il CERT Sogei svolge in collaborazione con il SOC e le strutture IT di riferimento, finalizzata all'estrazione di indicatori e allo sviluppo di metodologie di protezione avanzata. In particolare, gli sforzi sono stati indirizzati verso la realizzazione e l'implementazione di progetti di protezione per il contrasto dei ransomware.

Per rafforzare la consapevolezza dei propri utenti, il CERT Sogei ha avviato in collaborazione con le strutture aziendali di gestione e formazione del personale, un programma di cyber security awareness suddiviso in due fasi: la prima consiste in una survey finalizzata a rilevare il livello di sensibilità e di conoscenza dei rischi cyber e la capacità di riconoscere possibili attacchi (per esempio e-mail di phishing), la seconda consiste nell' integrare eventuali carenze con sessioni formative ad hoc tramite moduli e-learning interattivi. Questo ha rafforzato la consapevolezza degli utenti e il ruolo del CERT Sogei, come punto di riferimento di queste tematiche, dando indicazioni di comportamento a fronte di dubbi o anomalie. Il CERT Sogei svolge regolarmente attività di analisi e di miglioramento delle proprie capacità di infosharing e identificazione preventiva delle possibili minacce.

Ad oggi sono stati coinvolti nel programma pilota circa cento dipendenti. Il piano di attività 2018 prevede l'estensione del programma agli oltre 2.000 dipendenti Sogei, ad un campione di utenti dei Clienti istituzionali e l'estensione a circa 40.000 utenti nel 2019.

Per rafforzare la risposta alle minacce cyber verso le proprie infrastrutture la Sogei ha, inoltre, sottoscritto convenzioni con il CNAIPIC, il DIS e altri enti al fine di collaborare e condividere le informazioni consolidando le capacità di analisi interne attraverso l'identificazione di indicatori rilevanti.

Nel corso del 2017 è stato avviato un programma al fine di individuare una soluzione che potesse unire una piattaforma di cyber threat intelligence di mercato con i flussi e le attività di analisi del CERT Sogei. Nel corso del 2018

si procederà all'avvio della soluzione che comprenderà componenti sviluppate internamente al fine di poter permettere agli analisti di non disporre semplicemente di un feed di threat intelligence (principalmente OSINT), ma di una piattaforma di analisi e correlazione con il resto dell'infrastruttura aziendale. I risultati di tale attività permetteranno di creare flussi informativi verso le strutture di security governance e compliance aziendali al fine di migliorare l'analisi del rischio tramite la fornitura di dati relativi agli eventi occorsi nelle varie aree e servizi aziendali. Contestualmente saranno migliorati i flussi informativi verso i clienti e la Constituency, per tenere informati i vari referenti e responsabili dei servizi erogati da Sogei per conto dell'Amministrazione sullo stato di gestione degli incidenti e su possibili eventi e minacce.

La direttrice metodologica che continua a guidare le attività del CERT Sogei è volta a seguire un percorso di evoluzione delle capacità operative di un CERT/CSIRT da response a readiness, come indicato dalle normative nazionali e internazionali.

Molto dovrà essere ancora fatto a livello nazionale specialmente per recepire le indicazioni riguardanti la creazione di un punto di coordinamento e diffusione centralizzato delle informazioni, la necessità di avere dei livelli di sicurezza omogenei tra PA al fine di poter identificare carenze o possibili vettori di attacco e l'attivazione di processi chiari e attuabili per la gestione di un incidente di alto impatto sul sistema paese.

Il CERT Sogei proseguirà la propria attività di sviluppo, predisponendosi alle nuove sfide per la sicurezza cibernetica nazionale e aumentando la propria capacità di risposta agli eventi occorsi sulla infrastruttura gestita, in linea con il ruolo di partner tecnologico del MEF e hub strategico della PA digitale.

L'EVOLUZIONE DEI PRESIDI DI SICUREZZA CYBER NEL SETTORE BANCARIO ITALIANO: L'INIZIATIVA CERTFIN[5]

a cura di **Monica Pellegrino**, ABI Lab

La trasformazione digitale è un fenomeno che sta coinvolgendo la nostra società, cambiando le abitudini e i comportamenti quotidiani sia dei cittadini che delle imprese. Il settore bancario sta lavorando attivamente per rispondere alle esigenze che sopraggiungono dal mutamento dell'ecosistema digitale che vede tutti gli attori sempre più interconnessi tra loro, con servizi evoluti, fruibili da più device e veloci.

In questo contesto in continuo mutamento, emergono nuovi scenari di rischio

[5] Questo articolo è tratto dall'*Annual Report 2017* di FPA

cyber, con impatti potenzialmente di ampia portata. Fin da subito il settore bancario ha maturato la consapevolezza e la lucidità di far evolvere l'approccio alla gestione della sicurezza, conscio della complessità delle minacce informatiche e del fatto che proprio la forte interconnessione e interdipendenza che esiste nel mondo digitale tra banche, infrastrutture di mercato, utenti finali, fornitori e provider esterni, può far sì che un attacco cyber si propaghi a valanga da un punto a un altro della rete con estrema rapidità.

Un importante passo avanti a livello di settore, in tema di sicurezza informatica, è stato effettuato il 20 dicembre 2016, quando la Banca d'Italia, l'Associazione bancaria italiana (ABI) e il Consorzio ABI Lab hanno firmato una convenzione per rafforzare la collaborazione sulla cybersecurity. L'accordo ha previsto la realizzazione del **CERTFin (Computer Emergency Response Team Finanziario Italiano)**, una struttura altamente specializzata, basata sul principio della cooperazione tra pubblico e privato e dedicata al settore finanziario italiano, che ha l'obiettivo di prevenire e contrastare le minacce informatiche legate allo sviluppo delle nuove tecnologie e dell'economia digitale. L'iniziativa garantisce una **capacità di risposta e di prevenzione più coordinata** rispetto al passato e rappresenta un'arma di difesa in più per il sistema finanziario rispetto alle minacce cyber, partendo dal presupposto che la lotta al crimine e agli attacchi cyber non può che essere un obiettivo comune.

Per quanto riguarda la gestione dell'iniziativa, le decisioni strategiche e di indirizzo sono affidate a un Comitato Strategico presieduto dalla Banca d'Italia e dall'ABI, mentre i servizi sono coordinati dalla Direzione Operativa gestita dal Consorzio ABI Lab e messi a disposizione dei partecipanti su base cooperativa, grazie al coinvolgimento degli operatori bancari e finanziari italiani. **La partecipazione è aperta su base volontaria a tutti gli operatori del settore**: banche, prestatori di servizi di pagamento, intermediari finanziari, infrastrutture e società di mercato, gestori di infrastrutture tecnologiche e di rete, soggetti assicurativi e altre autorità di settore.

In linea con la mission prefissata, dal 1° gennaio 2017 il CERTFin svolge il compito di raccogliere dati, indicazioni e segnalazioni e di **analizzare tutti i fenomeni connessi all'universo della cybersecurity**, consentendo l'efficace scambio di informazioni tra gli operatori bancari e finanziari attivi in Italia e, allo stesso tempo, offrendo loro una serie di strumenti e servizi utili a rafforzare ulteriormente i presidi di sicurezza e garantendo al contempo la riservatezza delle informazioni scambiate. Inoltre, in coerenza con la strategia nazionale per la sicurezza cyber, il CERTFin si pone l'obiettivo di svolgere una funzione di raccordo con tutte le altre iniziative istituzionali avviate in Italia sui temi di sicurezza e protezione delle infrastrutture critiche, consolidando la collaborazione e ampliando ulteriormente la rete di interlocutori istituzionali e di esperti a livello nazionale e internazionale.

Le attività del CERTFin si incanalano in tre filoni operativi: in primo luogo, il **Financial Info Sharing and Analysis Center (FinISAC)**, cioè lo scambio sistematico di informazioni su minacce, vulnerabilità e incidenti e l'analisi delle possibili contromisure, effettuato anche attraverso la sistematizzazione e la contestualizzazione di informazioni tecniche, da parte del CERTFin, provenienti da più fonti di intelligence. La seconda area operativa è la creazione di un **Osservatorio denominato Cyber Knowledge and Security Awareness**, cui partecipano i referenti della constituency, che svolge attività di approfondimento delle minacce, analisi dell'evoluzione del contesto normativo, promozione di campagne di sensibilizzazione sulle tematiche di cybersecurity e partecipazione a esercitazioni e simulazioni a livello nazionale e internazionale. Terzo e ultimo filone è legato al ruolo di **Centrale operativa di gestione delle emergenze cyber**, che prevede attività di analisi e coordinamento in caso di emergenze e incidenti di rilevanza per il settore, oltre che di condivisione delle strategie di risposta più appropriate.

Grazie all'attività del CERTFin è quindi possibile rendere ancora più tempestiva e omogenea la circolazione delle informazioni sugli eventi e sui fenomeni che riguardano la sicurezza informatica e rafforzare la capacità di intelligence e awareness del settore bancario e finanziario sui fenomeni cyber, con conseguenti impatti positivi per l'intero Sistema Paese.

FOCUS ON: PA E *MOBILE SECURITY*

SPUNTI PER UNA POSSIBILE LINEA GUIDA IN TEMA DI SICUREZZA IN MOBILITÀ

INTRODUZIONE

Il tema della *mobile security* è sempre più attuale e pervasivo, vista la diffusione di smartphone e device mobili, ormai diventati di uso comune. Una tendenza che si va progressivamente affermando anche in ambito PA, soprattutto alla luce dell'emergere di nuovi trend, quali l'introduzione di nuove modalità di lavoro in mobilità (es. *smart working*) e la progressiva diffusione dell'approccio Byod (*Bring your own device*), con la conseguente creazione di contesti "promiscui", in cui l'ambiente personale e l'ambiente professionale coesistono sullo stesso apparato, e con l'esponenziale aumento delle tipologie di device con cui i sistemi informativi dell'organizzazione devono confrontarsi.

I dispositivi di mobilità sono sempre più spesso gli *end-point* attraverso il quale avvengono le interazioni tra il funzionario della PA e le piattaforme di gestione dei servizi. Nel prossimo futuro, è pertanto lecito attendersi un aumento esponenziale degli attacchi rivolti a questi dispositivi, ormai fonti incredibili di dati e informazioni sensibili, afferenti tanto alla vita personale del dipendente quanto al proprio ente di appartenenza.

Occorre quindi spostare il focus della sicurezza all'interno delle organizzazioni pubbliche, passando da forme più tradizionali di difesa del perimetro della rete aziendale ad approcci più focalizzati sulla protezione delle informazioni a 360 gradi[6].

Da qui l'esigenza di sviluppare alcuni possibili spunti utili a definire un'ipotetica linea guida in tema di sicurezza mobile nella pubblica amministrazione. Il contributo non ha ovviamente pretese di esaustività, ma si pone l'obiettivo di stimolare ulteriori riflessioni ed approfondimenti, a partire dalla prossima edizione del Cantiere.

[6] Cfr. Fabio Bucciarelli, Rapporto Clusit 2017

ELEMENTI DI RIFLESSIONE: IL CONTRIBUTO DEL CANTIERE

a cura di **Antonio Bosio** (Samsung), **Fabio Bucciarelli** (Regione Emilia Romagna) e **Gianluca D'Acunzo** (GSE)

Domanda di partenza: come rendere i terminali mobili più sicuri e adatti al contesto evolutivo della PA?

Punto di partenza: i device mobili rappresentano oggi un fondamentale strumento di lavoro del dipendente pubblico

Criticità riscontrata: mancanza e/o frammentazione di requisiti di riferimento, sulla base dei quali sviluppare capitolati di verifica/test che possano:

- guidare lo sviluppo dei terminali futuri
- consentire la validazione delle implementazioni effettuate di volta in volta dai fornitori
- qualificare il device che viene utilizzato, sia quando fornito dalla PA che quando reso disponibile dal dipendente stesso

Tali requisiti contribuirebbero all'innalzamento qualitativo dell'intera industria di settore, spingendola in direzione di una maggiore sicurezza.

Ad oggi le possibilità di erogare servizi da parte della PA verso i propri collaboratori/dipendenti sono due: device utilizzati come elementi attivi della infrastruttura di rete oppure device utilizzati come semplici elementi passivi.

Device come elemento attivo

I terminali mobili sono utilizzati mettendo a valore le loro caratteristiche peculiari quali ad esempio la potenza di calcolo, i sensori, interazione profonda ed ottimale tra app/servizi e l'HW/sensori del dispositivo, la visualizzazione auto-adattativa, la capacità di gestire processi off-line in assenza di connettività e risincronizzarsi quando questa torna ad essere disponibile (funzionamento asincrono).

Si evidenziano in particolare i seguenti punti di attenzione:

- ***sicurezza del dispositivo*** - 12 punti per la sicurezza dei dispositivi (**https://www.ncsc.gov.uk/guidance/end-user-devices-security-principles**):

    1. Protezione dei dati in transito da e verso il dispositivo
    2. Protezione dei dati che risiedono sul dispositivo
    3. Autenticazione e autorizzazione (User to device, User to service, Device to service) basata anche su dati biometrici (fingerprint, scansione retina)

4. Secure boot
5. Platform Integrity e Sandbox delle applicazioni
6. Whitelist delle applicazioni
7. Malicious code detection and prevention
8. Security policy enforcement
9. External interface protection
10. Aggiornamenti di sicurezza del SO del dispositivo
11. Event collection per analisi eventi critici sulla sicurezza del dispostivo
12. Incident response

- ***gestione del doppio ambiente personale/lavorativo (segregazione ambienti)***

La segregazione dell'ambiente di lavoro da quello privato sul singolo dispositivo consente all'azienda di avere pieno controllo sulla gestione della conformità, di seguito le raccomandazioni a seconda dello scenario d'utilizzo:

1. Gli utenti utilizzeranno il contenitore tutte le volte che svolgeranno attività che prevede l'utilizzo di dati sensibili e la piattaforma esterna per tutte le altre attività.
2. Le applicazioni e i dati aziendali dovrebbero essere tenuti all'interno del contenitore, ove possibile.
3. La separazione dell'ambiente professionale da quello personale concilia il logging sugli strumenti professionali con il pieno rispetto della privacy necessaria rispetto all'ambiente personale

- ***gestione da remoto dei dispositivi, inclusi blocco e cancellazione di tutti i dati aziendali***

- ***gestione degli aggiornamenti Firmware del terminale***

- ***rilascio di app e servizi in ambiente privato***

La cosa più importante nella scelta di un prodotto di Enterprise Mobility Management (EMM) è sceglierne uno che indirizzi le specifiche esigenze aziendali. Questa decisione sarà diversa per tutti, il che significa che non è sufficiente scegliere un particolare prodotto solo perché un altro dipartimento od organizzazione lo ha fatto.

Quindi un elemento importante è la fase iniziale di definizione dei requisiti, partendo da considerazioni sulla sicurezza.

Device come elemento passivo

I terminali mobili sono in questo caso utilizzati solo per funzionalità di Remote Desktop o Virtual Desktop, ottenute per mezzo di una VPN. Rispetto allo

scenario di una maggiore integrazione, è evidente come il fatto che nessun dato venga memorizzato sul dispositivo produca una apparente semplificazione. Tuttavia, a causa del fatto che app e servizi non interagiscono in maniera ottimale con l'HW, l'esperienza d'uso degli utenti diventa accettabile solo con display di dimensione pari almeno a 10 pollici. Dimensioni inferiori del display non sono adatte ad un utilizzo Virtual Desktop.

La gestione remota del dispositivo è comunque raccomandata anche in questo caso per evitare che eventuali sessioni in esecuzione al momento dello smarrimento, e/o password di accesso non particolarmente robuste, possano rappresentare un varco verso l'infrastruttura.

L'utilizzo come mero device di accesso non consente di sfruttare a pieno le peculiarità HW e SW del dispositivo e le prestazioni di lavoro dipendono esclusivamente dalla disponibilità e dalla qualità della connessione di rete. Per avere una esperienza utente accettabile è necessario **disporre di una connessione affidabile a bassa latenza al sistema remoto.**

Configurazioni di questo tipo rendono inoltre difficile l'utilizzo di HW locale, integrato o esterno al dispositivo.

Inoltre, sebbene l'approccio passivo basi la sua apparente robustezza sul fatto che nessun dato venga memorizzato nel dispositivo, il livello di sicurezza del terminale non è affatto secondario: eventuali malware che dovessero effettuare il keylogging o lo screen capturing potrebbero operare indisturbati e raccogliere informazioni rilevanti.

Approccio Bring Your Own Device

È importante comunicare la propria politica BYOD aziendale verso i dipendenti, è auspicabile prevedere la formazione del personale in modo che venga recepita la responsabilità nell›uso aziendale di dispositivi personali.

Opportuno effettuare da parte della PA una pre-selezione dei dispositivi abilitati alla modalità BYOD sulla base degli elementi indicati al punto "Sicurezza del dispositivo" e rendere noto ai dipendenti l'elenco dei modelli abilitati. La gestione dei terminali senza pre-selezione espone a rischi relativi alla sicurezza e aumenta esponenzialmente il carico di lavoro sul team IT.

Governance

Rispetto alla **dimensione della governance**, si evidenziano i seguenti punti di attenzione:

- definizione chiara della responsabilità di gestione dello smartphone e dei

device di servizio poi rilasciato a dipendenti e dirigenti per poter approntare le necessarie contromisure in caso di problema
- superamento del concetto di smartphone come puro strumento di fonia o addirittura afferente ai servizi di sede, e transizione verso gestione comune ai sistemi informativi gestionali
- definizione di policy per i dipendenti, sia per ciò che riguarda i device forniti dall'ente, sia nel caso di device personali (**disciplinari** con responsabilità rilanciata sull'utente)
- azioni di formazione e sensibilizzazione dei dipendenti e dei vertici sulle minacce cyber via mobile (servizi interni, app, whatsapp, ecc.), insistendo anche sui rischi personali, e non solo aziendali, di un utilizzo non appropriato
- gestione del portafoglio app

I PROTAGONISTI DEL CANTIERE

Andrea Rigoni
Partner Cyber Security - Deloitte Risk Advisory

Fabio Bucciarelli
Responsabile Sicurezza informatica, Regione Emilia Romagna

Marina Apicella
B2B Channel Account Manager - Public Sector Samsung Electronics

Giancarlo Buzzanca
Responsabile Area sviluppo applicazioni web/informatiche, sicurezza informatica, Ministero dei Beni, delle Attività Culturali e del Turismo

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

Alessandra Camporota
Responsabile Ufficio per la transizione al digitale, Ministero dell'Interno

Angelo Luca Barba
già Head of Marketing Cyber Security, Intelligence & Digital Infrastructures, Leonardo

Giancarlo Cecchetti
Responsabile Area Sistemi e Reti, Umbria Digitale

Antonio Bosio
Product & Solutions Director, Samsung Electronics

Massimiliano Chiardoni
Responsabile Area Cyber Security, SOGIN

Gianluca D'Acunzo
Responsabile Sicurezza Informatica, Gestore dei Servizi Energetici – GSE

Fabrizio Gergely
Manager Systems Engineering Enterprise & Public Sector Italy, Cisco Italia

Sergio De Paola
già Dirigente Divisione Gestione Sistemi, Infrastrutture e sito internet, DGSIS, Ministero delle Infrastrutture e dei Trasporti

Stefano Giannandrea
Responsabile Area Monitoraggio Qualità & Sicurezza, Lepida

Francesco Di Maio
Capo Dipartimento Sicurezza, ENAV

Andrea Guarino
Responsabile Security, Privacy & Compliance, ACEA Spa

Stefano Diofebi
Capo del Centro Sicurezza Telematica – Ce.Si.T., Comando Generale, Arma dei Carabinieri

Fabio Lazzini
Responsabile Security Governance e Privacy, Sogei

Rita Forsi
Direttrice ISCOM - Istituto superiore delle comunicazioni e delle tecnologie dell'informazione, Ministero dello Sviluppo Economico

Marco Manini
Capo dell'ufficio per la gestione dei sistemi informatici, Servizio Informatica, Senato della Repubblica

Alessandro Fontana
SI Alliance Manager, Trend Micro

Sandro Mari
CERT Nazionale, Istituto Superiore delle Comunicazioni, Ministero dello Sviluppo Economico

Leandro Gelasi
Responsabile Settore IT Operations, Corte dei Conti

Diego Mezzina
Responsabile IT Security, INSIEL

Benito Mirra
Cyber Security Officer, Huawei Enterprise Business Group

Salvatore Renato Naro
ICT Specialist, Ministero della Difesa

Giorgio Mosca
Responsabile Analisi Competitiva, Strategie e Tecnologie – Divisione Security & Information Systems, Leonardo

Giovanni Mellini
Security Engineer & Architect, ENAV

Gastone Nencini
Country Manager, Trend Micro Italia

Vincenzo Pensa
Responsabile Direzione Sistemi Informativi ed Innovazione, ACI - Automobile Club d'Italia

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

Rosario Riccio
Dirigente Ufficio 4 Servizi Infrastrutturali e di rete, D.G. Contratti, Acquisti, Sistemi Informativi e Statistica, Ministero dell'Istruzione, dell'Università e della Ricerca

Giuseppe Rutigliano
Capo del CERT, Comando Generale Arma dei Carabinieri

Pierluigi Sartori
Responsabile Cybersecurity, Informatica Trentina

Mario Terranova
Responsabile Area CERT PA, Agenzia per l'Italia Digitale

Enzo Veiluva
Responsabile Sicurezza ICT & Privacy, CSI Piemonte

Domenico Vulpiani
già Responsabile Unico Centro Elaborazione Dati, Ministero dell'Interno


FPA
DIGITAL360


cisco


DXC.technology


HUAWEI


LEONARDO


SAMSUNG


TREND
MICRO
Securing Your Journey to the Cloud