

IL LAVORO FEMMINILE NELLA SICUREZZA DIGITALE IN ITALIA

Considerazioni dal Rapporto 2020 CSWI e dalla Tavola Rotonda alla quale hanno partecipato donne attive nel campo della sicurezza digitale. Il webinar disponibile su Youtube. a pag.20

CYBER ATTACK

CYBER CRIMINALI ASSASSINI SFRUTTANO IL COVID-19

a pag.04

IN QUESTO NUMERO:

CYBER ATTACK

pag. 04-05

Cyber criminali assassini sfruttano il covid-19 4-6

pag. 07-08

I punti critici della sicurezza del cloud

pag. 09-10

La business continuity inizia da una solida sicurezza

SOLUZIONI

pag. 11-13

Costruire un SOC per le infrastrutture critiche in 3 fasi

pag. 14

La piattaforma di sicurezza Cisco SecureX vince la complessità

pag. 15

Kaspersky informa in tempo reale sulle minacce

pag. 17

Email più sicure con l'intelligenza artificiale di Darktrace

pag. 18

Zscaler si espande e migliora la security nel cloud

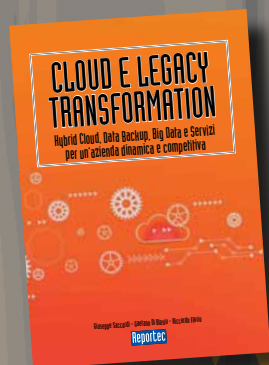
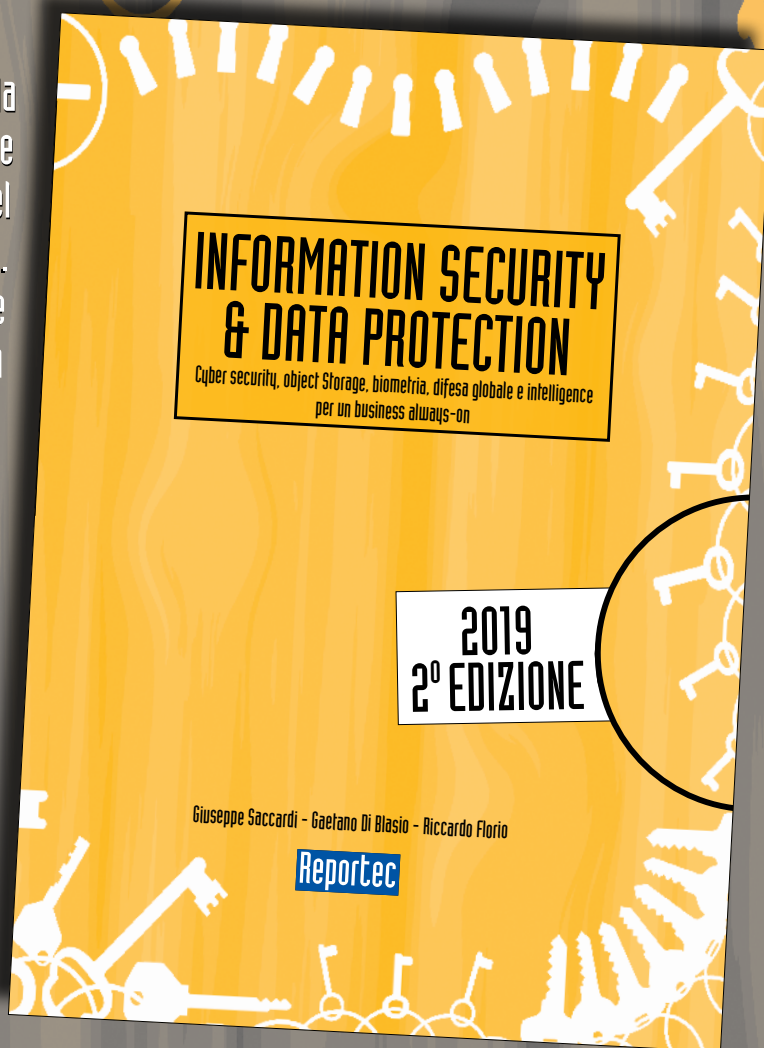
SPECIALE

pag. 20-23

Il lavoro femminile nella sicurezza digitale in Italia

È disponibile il nuovo libro **SICUREZZA E PROTEZIONE DEI DATI**

In oltre 200 pagine il punto sulla situazione della cybersecurity e sulle dinamiche aziendali nella protezione del dato e della continuità del business. Una tematica sempre più vitale per le imprese, le quali devono mettere in conto che saranno attaccate. Ormai esistono sistemi automatici e pressioni da parte dei cybercriminali, tali per cui nessuno può sentirsi al sicuro: chi non è ancora stato attaccato lo sarà e, se non subirà danni gravi, sarà solo perché chi l'ha assalito cercava qualcos'altro.



È disponibili anche
CLOUD E LEGACY TRANSFORMATION

Il libro è acquistabile al prezzo di 30 euro (IVA inclusa) richiedendolo a
info@reportec.it - tel 02 36580441 - fax 02 36580444

Security & Business 52
aprile 2020

Direttore responsabile:
Gaetano Di Blasio

In redazione:
Giuseppe Saccardi, Paola
Saccardi

Hanno collaborato:
Riccardo Florio

Grafica: Aimone Bolliger
Immagini: dreamstime.com
www.securityebusiness.it

Editore: Reportec srl
Via Marco Aurelio 8
20127 Milano
tel. 02.36580441
Fax 02.36580444
www.reportec.it

Registrazione al tribunale
n.585 del 5/11/2010

Tutti i marchi sono
registrati e di proprietà
delle relative società

Da War Games all'omicidio

Il film di John Badham del 1983 fu il primo a sollevare l'importanza della sicurezza informatica. Il giovane David, interpretato da Matthew Broderick ingaggia quello che crede un gioco con un computer militare e rischia di scatenare una guerra.

Oggi la guerra informatica viene combattuta quotidianamente da fronti contrapposti. La guerra che ci coinvolge tutti ha diverse sfaccettature, ma diventa sempre più difficile considerarle una questione etica.

In particolare, scomparso il gioco goliardico degli hacker ante litteram, gli esperti della sicurezza informatica si distinguono tra black e white hat, ma non sempre il bianco e nero è ben marcato, qualche sfumatura di grigio traspare sempre. Fino a che punto ci si può considerare un "ethical hacker" ?

Il cybercrime ha decisamente mostrato un indole criminale che non è possibile distinguere dal delinquente comune armato di pistola, anzi, a differenza dei duelli del Far West, lo scenario è drammaticamente più subdolo.

L'emergenza Coronavirus ha dimostrato che esperti informatici privi di qualsiasi etica morale sono pronti a uccidere. L'ospedale di Brno, nella repubblica Ceca è stato attaccato e costretto a spostare in altre strutture i pazienti critici, mettendo a rischio la loro vita.

Occorre affrontare la questione per quello che è, altrimenti i cyber criminali potranno agire indisturbati, celandosi dietro server "fantasma" in nazioni compiacenti.

Nel numero 52 di Security e business trovate un breve resoconto dell'Ocse sugli attacchi di febbraio e marzo riconducibili all'emergenza Corona virus.

Peraltro, è importante sottolineare che gli attacchi vanno contrastati con mezzi adeguati, non necessariamente con enormi investimenti, ma dei budget per la security occorre stanziarli. Una ricerca di Fortinet, per esempio, mostra che quasi due terzi delle aziende mancavano di personale qualificato per mantenere efficaci le security operations già prima dei recenti avvenimenti. Ora, a causa delle disposizioni in merito al distanziamento sociale, il numero di dipendenti che si occupano di sicurezza risulta ulteriormente ridotto.

Nella rubrica Cyber Attack, come di consueto, trovate altri dati sulla sicurezza, come quelli del Cisco 2020 CISO Benchmark Study. A seguire le soluzioni più recenti e, a chiudere il numero lo speciale legato al rapporto di AIPSI sul Lavoro al Femminile nella Cyber Security, accompagnato dalla tavola rotonda che si è tenuta il 21 Aprile 2020.

CYBER CRIMINALI ASSASSINI SFRUTTANO IL COVID-19

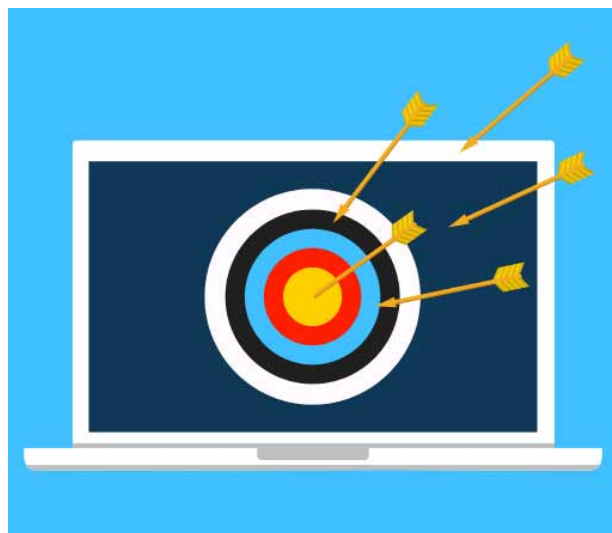
L'Ocse lancia un allarme sicurezza digitale e fisica causato dagli attacchi contro gli ospedali: non aprite quella mail

di Gaetano Di Blasio

L'Organizzazione per la Cooperazione e lo Sviluppo Economico ha diffuso un parziale resoconto degli attacchi di varia forma che sono andati crescendo con l'avvento della pandemia, cercando di far crescere la consapevolezza sui rischi informatici e contrastare l'attacco di massa senza precedenti sul fronte digitale che sfrutta la paura e l'interesse per informazioni riguardanti il Coronavirus.

Innanzitutto non aprite mail sospette e non cliccate su alcun link la cui provenienza non sia sicura al 100%.

Cyber criminali senza scrupoli né dignità hanno acuito la pressione di attacchi informatici verso strutture ospedaliere e ovunque si concentrasse l'interesse sulla pandemia in corso. Non si può dire con certezza, ma neanche escludere che il blocco di apparati o alcuni dei ritardi nei sistemi informatici e medicali abbia causato la morte di un paziente, ma, in ogni caso sarebbe potuto accadere, eppure i criminali non si sono fermati, pertanto hanno volontariamente accettato di poter uccidere un malato, come nel caso di un paziente di terapia intensiva che è stato necessario trasferire da un ospedale a un altro.



Molti gli attacchi DDoS contro la sanità

Un bollettino di guerra

Dal febbraio 2020, si è riscontrato un aumento delle campagne di phishing basate su contenuti COVID-19, fra le quali: email con un tema coronavirus nel campo dell'oggetto o come nome file allegato, e-mail o SMS che rappresentano il governo in Australia e nel Regno Unito; e-mail che impersonano leader o istituzioni, come l'Organizzazione Mondiale della Sanità; e-mail, collegamenti o applicazioni Web che imitano iniziative legittime, per esempio umanitarie.

Non tutti gli attacchi sono stati della stessa gravità, anche perché sono state impiegate diverse tecniche.

Per esempio è stato compromesso il cruscotto interattivo della Johns Hopkins University, che tracciava

i contagi. Più precisamente, è stato creato un sito fake sul quale era installato un malware che rubava password. Il kit per creare tale sito è disponibile online nel dark Web: costa 200 dollari, secondo l'Ocse. Una campagna di posta elettronica rivolta alle industrie sanitarie e manifatturiere degli Stati Uniti all'inizio di marzo 2020 ha fatto leva su un progetto reale e legittimo di calcolo distribuito per la ricerca sulle malattie. L'e-mail chiedeva ai destinatari di installare un allegato allo scopo di aiutare la ricerca per trovare una cura contro il coronavirus. L'allegato conteneva malware che rubava credenziali e "portafogli" di cripto valuta archiviati offline.

Anche smart working e didattica a distanza a rischio

I criminali informatici stanno anche sfruttando la popolarità di strumenti utilizzati per il lavoro e la didattica a distanza, quali Zoom per la videoconferenza. Gli esperti coinvolti dall'Ocse, hanno individuato campagne di phishing con allegati dannosi contenenti zoom nel nome del file e o nel titolo. Oltre 1700 nuovi nomi di dominio Zoom sono stati registrati sin dall'inizio della pandemia, probabilmente per uso dannoso. Altri esempi comprendono nuovi domini mascherati da sito legittimo di Google Classroom.

L'ospedale Universitario di Brno è stato costretto dal governo Ceco ad accrescere la sicurezza

Omicidio colposo o tentato omicidio?

Come accennato, ci sono stati anche casi di attacchi ransomware e DDoS contro attività essenziali come ospedali in Francia, Spagna e Repubblica Ceca. Qui, in particolare il secondo più grande ospedale, quello universitario di Brno, è stato attaccato il 12 e 13 marzo, causando un arresto immediato dei computer costringendo la struttura ad annullare le operazioni e trasferire pazienti acuti in altri ospedali. Per questo l'ospedale è stato costretto dal governo ceco, e con lui altre strutture sanitarie del Paese, a migliorare la sicurezza dei principali sistemi ICT. Se durante il trasferimento il paziente fosse deceduto, come si sarebbe dovuta classificare la sua morte? I cyber criminali sono, evidentemente disposti a uccidere. Un'ulteriore considerazione riguarda la responsabilità delle strutture sanitarie.

A Parigi un ospedale ha dovuto fronteggiare un attacco DDoS di un'ora e mezza, domenica 22 marzo,



paralizzando due indirizzi Internet, fortunatamente senza coinvolgere gli apparati medici.

In Spagna, un attacco ransomware è stato lanciato contro le istituzioni sanitarie il 23 marzo 2020. Altri DDoS registrati negli USA il 15 e il 20 marzo.

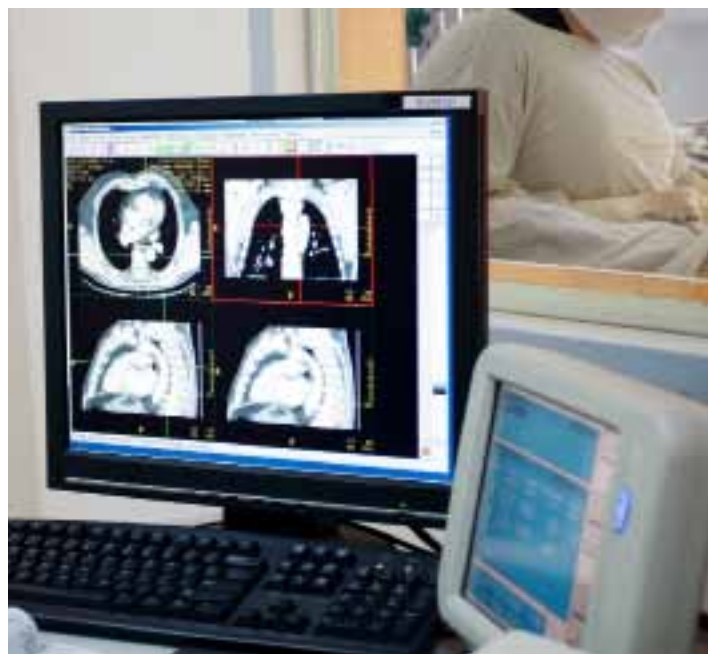
In Francia a Marsiglia, invece, il sistema informativo del governo locale ha dovuto affrontare un attacco di ransomware il 14 marzo, alla vigilia delle elezioni locali: tutte le applicazioni rivolte al pubblico, nonché diversi sistemi interni, sono andati offline.

Accrescere l'attenzione alla sicurezza informatica

Purtroppo i cyber criminali sanno benissimo che le persone, ma anche i dipartimenti marketing di alcune aziende sono più sensibili nei momenti di stress e crisi e facilmente possono cadere nelle trappole dei cybercriminali che nascondono truffe e attacchi ransomware, bloccando o degradando le prestazioni dei sistemi informatici.

Occorre adottare comportamenti accorti, cioè prassi aziendali che blocchino o riducano sensibilmente il rischio di compromettere la sicurezza. Al riguardo l'Ocse sta avviando programmi di sensibilizzazione supporto per le organizzazioni vittime nonché sistemi di monitoraggio. Inoltre, mettono in guardia gli esperti, molti degli incidenti potrebbero essere evitati, poiché si tratta di software maligni noti.

La "Cyber and Infrastructure Security Agency" (CISA) degli Stati Uniti ha creato sul proprio sito Web una sezione interamente dedicata ai rischi per la sicurezza legati alla crisi COVID-19). Include avvisi e



raccomandazioni riguardanti campagne di truffa e phishing relative a COVID-19, indicazioni sul telelavoro e una nota sulla gestione dei rischi.

L'ENISA, insieme a CERT-EU ed Europol hanno avviato una collaborazione, prima del 20 marzo, tesa a tenere traccia delle attività dannose legate a COVID-19, avvisare le loro rispettive comunità e aiutare a proteggere i cittadini confinati a casa.

Il Canadian Centre for Cyber security ha dichiarato la pandemia il maggior rischio digitale.

Il processo di sensibilizzazione continua con alcune raccomandazioni:

1. Trattate con cautela e diffidate di qualsiasi messaggio (mail o post sui social) riguardante le notizie relative alla pandemia e alle parole chiave: coronavirus e Covid-19. accertate le fonti e non aprite link che non siano sicuri;
2. aggiornate gli strumenti informatici, specie quelli relativi allo smart working oltre a smartphone e altri dispositivi;
3. Eseguite regolarmente il backup dei contenuti, in particolare di dati importanti.



I PUNTI CRITICI DELLA SICUREZZA DEL CLOUD

Uno studio evidenzia la crescita degli investimenti in tecnologie per la sicurezza del cloud e l'automazione per ridurre la complessità

di Gaetano Di Blasio



Stefano Vaninetti - Security Leader Cisco Italia

È indiscusso che la trasformazione digitale costituisce un'opportunità per l'IT e i responsabili della sicurezza, poiché tramite essa le aziende possono innovarsi ed essere competitive, ma si tratta pur sempre di una trasformazione che costituisce un cambio significativo in termini di infrastruttura. Ed è un cambiamento che impone la necessità di contrastare minacce nuove e sofisticate.

Una complessità, evidenzia un recente studio, deriva dal fatto che in media un'azienda utilizza oltre 20 tecnologie per la sicurezza, pur se è in corso una fase di consolidamento verso un unico fornitore.

I dati evidenziano la situazione. Oltre il 90% dei CISO delle aziende italiane interpellate ha da 1 a

20 fornitori e oltre il 10% ritiene che gestire un ambiente pluri-fornitore risulti particolarmente impegnativo.

Ma cosa vien fatto per contrastare questa complessità? Non sorprendentemente, per migliorare la postura nei confronti della sicurezza, le aziende ricorrono ad una maggior sicurezza in cloud, per migliorare non solo la visibilità nelle reti, ma anche per favorire la collaborazione tra gli addetti alle reti, endpoint e sicurezza.

Ma quali sono le principali sfide e come sono percepite dai CISO e, come conseguenza, dove ritengono di dover intervenire, o sarebbe opportuno farlo?

Un primo punto è la protezione di dati e carichi di



lavoro e in questo un'infrastruttura cloud privata è ritenuta essere tra le principali sfide in termini di sicurezza. Altri punti critici sono la sicurezza della forza lavoro mobile (con oltre il 30% dei CISO che ritiene che i dispositivi mobile sono molto complessi da proteggere ma che tecnologie zero-trust possono essere di aiuto nel farlo), e la sicurezza dell'accesso alla rete (ma con però solo un 40% che ricorre per la protezione all'autenticazione multi-fattore per proteggere i dipendenti).

A fronte di queste criticità tre sono le tipologie di intervento messe in atto per mitigarle: una maggior collaborazione tra i team di rete e di sicurezza; il ricorso all'automazione, al machine learning e all'intelligenza artificiale; una maggior sicurezza del cloud in modo da ampliare la visibilità nella rete. Se questa è la situazione cos'altro si può fare per migliorare la sicurezza? Innanzitutto, suggeriscono gli esperti, è possibile adottare una difesa a più livelli, che dovrebbe includere interventi come quelli considerati e cioè un'autenticazione multi fattore, la segmentazione della rete e una migliore protezione degli endpoint, soprattutto per quanto riguarda l'utenza privilegiata.

Un secondo intervento può consistere nel migliorare i livelli di visibilità in modo da potenziare la governance dei dati e migliorare la conformità.

Di concreto aiuto nell'ottimizzare la strategia di sicurezza è poi l'implementazione un approccio zero-trust.



LA BUSINESS CONTINUITY INIZIA DA UNA SOLIDA SICUREZZA

Un'analisi di Fortinet evidenzia come la security automation costituisca una strategia efficace per garantirsi la business continuity

di Giuseppe Saccardi

L'emergenza sanitaria legata al COVID-19 non sta rallentando l'operato dei cybercriminali, che continuano a intensificare gli sforzi per trarre vantaggio da questa situazione.

Fortinet ha condotto un'analisi approfondita della tematica da cui si possono trarre spunti utili a garantire un alto livello di operatività anche lavorando da remoto.

La realtà è che quasi due terzi delle aziende mancavano di personale qualificato per mantenere efficaci le security operations già prima dei recenti avvenimenti. Ora, a causa delle disposizioni in merito al distanziamento sociale, il numero di dipendenti che si occupano di sicurezza risulta ulteriormente ridotto. In ogni caso i team, già sovraccarichi, sono impegnati nel risolvere una serie di nuove criticità, pur mantenendo costanti i controlli relativi alla sicurezza, anche da remoto.

“Anche se in questo momento molte realtà si stanno focalizzando, comprensibilmente, sui problemi di continuità aziendale, come la creazione di soluzioni ad hoc di smart working per i dipendenti, è bene non



distogliere lo sguardo dalla sicurezza. Questo aspetto, in particolare, è molto importante per quelle realtà che hanno un ruolo cruciale come gli ospedali e altri fornitori di infrastrutture critiche di primo e secondo livello, che non possono permettersi di sospendere le attività per un periodo di tempo prolungato”, commenta Spiega Antonio Madoglio, Director Systems Engineering Italy di Fortinet.

Per far fronte alle sfide che nascono dall'incremento del rischio e dal personale addetto alla sicurezza ridotto all'osso, suggerisce Fortinet, le aziende possono adottare una strategia di protezione, detection e response automatizzate.

Anche quando si ha a disposizione uno staff completo di professionisti della sicurezza informatica preparati, le minacce sono diventate così sofisticate e il tempo di esecuzione di un attacco è diventato così breve, che l'intervento umano non è più una strategia di sicurezza praticabile.

Automatizzare per proteggere

Automatizzando la protezione le aziende possono

disporre di informazioni in tempo reale relative allo stato della sicurezza che possono aiutare a identificare le minacce e a bloccarle tempestivamente.

La ricerca proattiva delle minacce e la correlazione automatizzata degli eventi possono impedire ai cybercriminali di sfruttare nuove vie di attacco.

Combinando il machine learning con le funzionalità di IA, è possibile esaminare continuamente nuovi file, siti web e infrastrutture di rete.

È così possibile identificare i componenti malevoli, oltre a generare in maniera dinamica una nuova threat intelligence che possa consentire alle aziende di prevedere e prevenire anche le future minacce informatiche.

Rilevare e correlare gli eventi

Un altro aspetto da considerare, osserva Fortinet, è che a causa dell'aumento degli attacchi avanzati, le minacce possono diffondersi rapidamente e quindi le reti necessitano di capacità di rilevamento avanzate. Ciò richiede un'architettura di sicurezza che consenta l'analisi unificata dei dati raccolti da diverse fonti d'informazione, compresi i log, le metriche riguardo alle performance, gli avvisi relativi alla sicurezza e le modifiche di configurazione.

Per la maggior parte delle aziende, tutto questo richiede capacità SIEM (acronimo di Security Information and Event Management), combinate con un motore di correlazione degli eventi distribuito per consentire il rilevamento di schemi di eventi complessi, in modo tale da abilitare una risposta in tempo reale.

I sistemi automatizzati consentono anche di dare priorità ad asset ed eventi, permettendo ai team di identificare rapidamente i problemi più critici che necessitano di un'analisi immediata.

Sfruttare il machine learning dà ai team che si

occupano di sicurezza la possibilità di rilevare comportamenti inusuali degli utenti senza richiedere agli amministratori di sistema di scrivere regole complesse.

Le funzionalità EDR (Endpoint Detection and Response) aggiunte ai dispositivi remoti consentono ai sistemi di sicurezza di rilevare e disinnescare le minacce in tempo reale, proteggendo l'endpoint stesso e prevenendo una potenziale violazione.

Un aiuto viene anche dalle nuove tecnologie di security orchestration, automation e response (SOAR), che permettono ai componenti separati tra loro di comunicare e lavorare insieme attuando un coordinamento difensivo per incrementare la visibilità.

Prevenire comporta vantaggi

Quello che si sta affrontando, osserva Fortinet, può essere un buon momento per una verifica delle pratiche di sicurezza. Possono essere inoltre messi in atto sistemi a prova di guasto, come ad esempio quelli che prevedono di operare in una modalità iniziale di solo monitoraggio per convalidare le risposte, prima di passare a un sistema completamente automatizzato. I benefici, nota l'azienda, superano di gran lunga i potenziali rischi. L'aggiunta dell'automazione alla strategia di sicurezza aumenta significativamente le possibilità di individuare una violazione o attività dannose, assicura risposte efficaci e tempestive e riduce al minimo i potenziali tempi di inattività dovuti alle violazioni.

Inoltre, consente alle risorse umane di lavorare su attività più impegnative mentre l'automazione delle attività manuali riduce le possibilità di un errore umano.

Aiuta anche a garantire che si continuino a soddisfare i requisiti di conformità durante i periodi in cui avvengono cambiamenti insoliti. ❖

COSTRUIRE UN SOC PER LE INFRASTRUTTURE CRITICHE IN 3 FASI

L'esperienza di Ukrenergo, operatore nazionale ucraino della distribuzione elettrica, che ha reso sicure le sue infrastrutture realizzando un SOC basato sulle soluzioni Micro Focus ArcSight

di Riccardo Florio

Ukrenergo è il gestore nazionale ucraino delle principali linee di distribuzione elettrica e di molte sottostazioni primarie. È interconnesso in modo sincronizzato con ENTSO-E, la rete europea degli operatori del sistema di trasmissione dell'elettricità, che rappresenta 43 operatori di 36 Paesi. L'esigenza di predisporre una protezione efficace contro i sempre più frequenti attacchi alle infrastrutture critiche ha portato l'operatore ucraino a realizzare un Security Operation Center (SOC) dotato delle soluzioni Micro Focus ArcSight.

«Negli ultimi due anni - spiega Dmitry Ryzhkov, senior information security analyst di Ukrenergo - l'Ucraina è

stata oggetto di diversi attacchi informatici. Il malware BlackEnergy ha interrotto l'attività di tre operatori regionali, Industroyer ha colpito una nostra sottostazione elettrica mentre GreyEnergy ha attaccato il settore energetico dell'Ucraina a Polonia. Inoltre, i ransomware WannaCry e Petya hanno colpito molte istituzioni governative e hanno interessato anche noi. Questi attacchi hanno determinato l'esigenza di predisporre una soluzione in grado di proteggerci per



La sede dell'azienda nazionale di energia elettrica Ukrenergo NPC a Kiev



Pierpaolo Ali, Director Southern Europe Security, Risk & Governance di Micro Focus

il futuro e abbiamo trovato questa soluzione nella realizzazione di un SOC dotato delle soluzioni Micro Focus».

Ukrenergio ha affrontato la realizzazione del SOC con una roadmap organizzata in tre fasi successive:

l'implementazione di una soluzione SIEM (Security Information and Event Management), la realizzazione di un pre-SOC per arrivare, infine, alla predisposizione del New Gen SOC vero e proprio.

«I più recenti dati sugli attacchi informatici - osserva Pierpaolo Ali, Director Southern Europe Security, Risk & Governance di Micro Focus - evidenziano come il settore delle infrastrutture critiche sia un target sempre più centrale per i cyber criminali, che richiede un approccio strutturato alla sicurezza. L'esempio di Ukrenergio dimostra come la gamma di soluzioni ArcSight, unita all'esperienza di Micro Focus nella gestione dei SOC, rappresenti un'opportunità per tutte le aziende che hanno l'esigenza di mantenere i propri sistemi critici disponibili e protetti».

Fase 1: SIEM

Il primo passo verso la realizzazione del SOC è stata l'implementazione della soluzione SIEM ArcSight Enterprise Security Manager (ESM), che ha previsto un periodo di formazione e apprendimento delle funzionalità del software.

L'utilizzo di ArcSight ESM ha permesso di avviare una fase di identificazione delle possibili vulnerabilità, di monitoraggio dell'infrastruttura e di analytics sugli eventi di sicurezza in modo da identificare i potenziali problemi; nel contempo, si è proceduto ad

ampliare progressivamente il numero di sistemi connessi al SIEM conseguendo un livello di visibilità sempre più dettagliato.

Questo tipo di analisi ha consentito a Ukrenergio di costruire uno "use

case" personalizzato per la propria infrastruttura.

«La prima cosa da fare - osserva Ryzhkov - è studiare la tua infrastruttura, comprendere come lavorano i tuoi sistemi IT, identificare le criticità e capire anche che tipologia di utenti hai. È anche molto importante stabilire un livello di comunicazione con le persone dell'IT e gli amministratori di rete, le cui esigenze in termini di visibilità, disponibilità e integrità potrebbero essere differenti da quelle di chi si occupa di sicurezza. È anche essenziale coinvolgere nel progetto tutte le figure aziendali, dall'help desk al management, perché diventi un obiettivo strategico condiviso da tutti. Infine, non va sottovalutata l'utilità delle community per condividere problemi e risolverli».

Fase 3: pre-SOC

Il secondo stadio della roadmap è servito a estendere e consolidare le modalità d'uso della soluzione SIEM. Il primo passaggio di questa seconda fase è stato di realizzare un audit interno per analizzare l'ambiente nella sua interezza, non solo a livello tecnologico, ma anche in relazione agli utenti.

Attraverso ArcSight FlexConnectors sono stati creati connettori personalizzati in grado di leggere e analizzare informazioni da dispositivi di terze parti e mappare tali informazioni su ArcSight. Questo ha consentito di acquisire eventi di sicurezza generati

da endpoint, dispositivi di rete, server, piattaforme cloud, security tool, scanner di vulnerabilità, fonti aggiuntive di Threat Intelligence e così via.

Sfruttando l'ampliato livello di visibilità Ukrenergo ha potuto realizzare "use case" più sofisticati, rafforzare le capacità di risk assessment e di intelligence sulle minacce, definire modelli di risposta agli incidenti, effettuare azioni di test e backup.

La realizzazione del SOC

Le capacità di intelligence e risk assessment sono state definite in modo completo con l'ultima fase, che ha avuto tre obiettivi primari.

Il primo obiettivo è stato definire i livelli in cui organizzare i ruoli degli operatori all'interno del SOC, assegnando le corrispondenti responsabilità.

Il SOC di Ukrenergo ha previsto un'organizzazione in quattro livelli. Al livello "tier 1" appartengono persone dedicate prevalentemente alle attività di monitoraggio e analisi degli eventi; il secondo livello riguarda chi svolge attività di analytics ed è coinvolto nei processi di coordinamento e risposta agli incidenti. A questi due livelli si sommano un livello di amministrazione dei sistemi e uno degli operatori con funzionalità avanzate.

Il secondo obiettivo ha riguardato l'interazione con il framework MITRE ATT&CK, la "knowledge base" di livello globale, accessibile gratuitamente, che mette a disposizione tattiche e tecniche di difesa, per comprendere metodi di attacco e sviluppare specifici modelli e metodologie di risposta alle minacce. Il framework supporta la governance, la gestione dei rischi, l'analisi del comportamento degli attaccanti,

la comprensione di come classificare e mitigare le minacce.

Ukrenergo ha implementato autonomamente tutti gli "use case" di MITRE ATT&CK, in aggiunta ai molti già nativamente messi a disposizione da ArcSight ESM. Il terzo e ultimo essenziale compito è stata l'implementazione della componente di analisi dei comportamenti per l'individuazione di situazioni anomale. «Un SOC non è fatto solo da strumenti - conclude Ryzhkov -. È un obiettivo che richiede molto tempo e che comprende anche Operation, manutenzione dei sistemi, formazione dei tecnici, relazioni sia all'interno del SOC sia con gli altri dipartimenti aziendali (soprattutto Management e IT). Collegare le sorgenti di eventi è un lavoro costante, che non ha fine perché il numero di compiti, processi e sistemi da connettere evolve costantemente. Per avere un SOC efficace in grado di evolvere rapidamente è anche essenziale predisporre un meccanismo per continuare a imparare e scoprire qualsiasi informazione rilevante (per esempio su attacchi e best practice) e condividerla rapidamente al proprio interno». ❖



LA PIATTAFORMA DI SICUREZZA CISCO SECUREX VINCE LA COMPLESSITÀ

Cisco SecureX è una piattaforma cloud che fornisce analisi approfondite e automatizza i flussi di lavoro, velocizza il rilevamento e la risposta alle minacce

di Giuseppe Saccardi

Man mano che le aziende intraprendono un percorso di trasformazione digitale, espandendosi verso il cloud, integrando l'IoT e l'accesso wireless ad alta velocità, aumenta la relativa superficie di attacco.

La protezione di questi ambienti diventa complessa a causa di tecnologie che non interagiscono tra loro. Ad esempio, lo studio Cisco2020 CISO Benchmark Study - effettuato su un campione di 2800 professionisti della sicurezza - ha riscontrato che il 28% degli intervistati ritiene che la gestione di un ambiente multi-vendor sia molto impegnativo, percentuale che è aumentata dell'8% rispetto al dato dell'anno scorso.

Per migliorare la protezione Cisco ha annunciato di aver semplificato radicalmente, con la sua nuova piattaforma SecureX, l'esperienza di utilizzo da parte dei clienti del proprio portfolio di soluzioni Cisco Security.

Cisco SecureX, di base, fornisce una user experience unica per tutte le soluzioni Cisco Security e per l'infrastruttura di sicurezza esistente dei clienti. In particolare, ha evidenziato la società, abilita una visibilità unificata, identifica le minacce sconosciute e automatizza i flussi di lavoro con l'obiettivo di rafforzare la sicurezza di reti, endpoint, cloud e applicazioni.

Tra le funzionalità di Cisco SecureX va annoverato:

- Visibilità unificata di tutto il portfolio di sicurezza dei clienti e delle soluzioni Cisco o di terze parti.

Cisco SecureX: ancora piu' valore per i clienti Cisco



© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

- Disponibilità di informazioni importanti per il business a clienti e partner in pochi dieci minuti, attraverso una soluzione cloud e multi-tenant.
 - Analisi approfondite di eventi e dati per l'intera infrastruttura inclusi gli endpoint, il traffico di rete proveniente da switch e router compreso quello cifrato, ambienti Google, AWS e Azure nonché gli ambienti data center privati.
 - Identificazione in pochi minuti degli obiettivi di un attacco, con la possibilità di risoluzione grazie all'utilizzo delle informazioni provenienti da prodotti di sicurezza e da feed di threat intelligence.
- «Oltre ai criminali informatici, anche la complessità è diventata un altro rischio che i team di sicurezza

devono affrontare e superare. Cisco SecureX rappresenta un cambiamento radicale nel modo in cui i clienti sperimentano la sicurezza, eliminando la complessità e fornendo una visione unificata sullo stato dei servizi di sicurezza e degli alert dei clienti. In questo modo, i team di sicurezza possono gestire le risorse in maniera più efficiente e rappresentare un fattore abilitante della trasformazione digitale», ha dichiarato Gee Rittenhouse, SVP e GM del Security Business Group di Cisco. ❖

KASPERSKY INFORMA IN TEMPO REALE SULLE MINACCE

Il vendor presenta il nuovo servizio di threat intelligence che fornisce avvisi in tempo reale sulle minacce rivolte ai clienti

di Paola Saccardi

Kaspersky ha annunciato un nuovo servizio Kaspersky Digital Footprint Intelligence che fornisce ai clienti aggiornamenti in tempo reale rispetto ai punti deboli della propria organizzazione.

Grazie a questo servizio, gli analisti di sicurezza di SOC e CERT possono migliorare la propria strategia di difesa in quanto possono sapere a quali informazioni sulla propria organizzazione i criminali

informatici potrebbero avere accesso e quali vettori di attacco potrebbero essere sfruttati.

Secondo l'indagine IT Security leaders condotto da 451 Research e commissionato da Kaspersky, la maggior parte dei CISO (64%) ha convenuto che velocità e qualità nella gestione dell'incident response siano le principali metriche per misurare le performance del loro lavoro.

Tuttavia, poiché un'azienda espone numerose risorse online, diventa più difficile per gli analisti della sicurezza tenere tutto sotto controllo e reagire alle minacce più significative in tempo.

Proprio per supportare le aziende in questo senso Kaspersky ha reso disponibile il nuovo servizio.

Individuare le minacce in tempo reale

Il servizio di Kaspersky offre la possibilità di capire quali sono le modalità di attacco dei criminali informatici ed anche quali informazioni siano facilmente raggiungibili da un attaccante.

Inoltre, offre alle aziende la possibilità di scoprire se la loro infrastruttura è già stata compromessa offrendo un'analisi sulle minacce mirate specificamente contro di loro.

Il servizio, spiega il vendor, si basa sugli insight degli esperti di Kaspersky che sono in grado di mettere insieme un quadro completo dello stato attuale degli attacchi rivolti ai clienti, identificando i punti deboli nel perimetro della rete, le minacce dei criminali informatici, le attività dannose e le fughe di dati.

L'inventario di rete, che utilizza metodi non intrusivi, identifica i componenti critici del perimetro di rete di un cliente, come i servizi di gestione remota, i servizi non intenzionalmente esposti e mal configurati e i dispositivi di rete.

In questo modo si ottiene una valutazione completa del rischio basata su una serie di parametri multipli, tra cui il punteggio base CVSS (Common Vulnerability Scoring System), la disponibilità di

exploit pubblici, l'esperienza di penetration testing dell'azienda e altre caratteristiche.

Inoltre i report di Kaspersky Digital Footprint Intelligence mettono in evidenza le attività dei criminali informatici rivolte anche contro i clienti, i partner e le infrastrutture dei fornitori e offrono una panoramica dei malware o degli attacchi APT in corso a livello di paese o verso un settore specifico.

Il servizio è disponibile nel Kaspersky Threat Intelligence Portal, un unico punto di accesso ai dati relativi ai cyber attacchi raccolti dall'azienda per oltre 20 anni e supportati da notifiche in tempo reale quando un report personalizzato viene aggiornato. Tramite una speciale API, Kaspersky Digital Footprint Intelligence può essere integrato con sistemi di gestione delle attività di terze parti.

Un occhio anche alle infrastrutture APT

Kaspersky Threat Intelligence Portal è stato anche potenziato con il nuovo APT C&C Tracking Service



che fornisce gli indirizzi IP delle infrastrutture connesse alle minacce avanzate. Questo aiuta gli analisti della sicurezza che lavorano nei CERT, nei SOC nazionali e nelle agenzie di sicurezza nazionali a monitorare l'implementazione di nuove infrastrutture dannose e ad adottare le misure necessarie per mitigare gli attacchi in corso e quelli futuri.

«I dati sono la linfa vitale per ogni azienda. Forniscono supporto alla costruzione di forti relazioni con gli stakeholders, al miglioramento dei prodotti per soddisfare le esigenze dei clienti e superare la

concorrenza. Qualsiasi incidente che influisce sulle informazioni sensibili, sia che si tratti di un attacco informatico mirato a rubare i dati dei clienti o alla fuga di segreti commerciali, può influire negativamente sulla reputazione di un'azienda e causare perdite finanziarie. Ecco perché abbiamo aggiunto una serie di nuovi servizi al Kaspersky Threat Intelligence Portal, in modo che i clienti possano tenersi aggiornati sulle minacce informatiche più rilevanti», ha commentato Sergey Martsynkyan, head of B2B product marketing at Kaspersky. ❖

EMAIL PIÙ SICURE CON L'INTELLIGENZA ARTIFICIALE DI DARKTRACE

Per contrastare l'incremento delle minacce alle mail cresce il ricorso ad una sicurezza basata sull'intelligenza artificiale di Darktrace

di Giuseppe Saccardi

Darktrace, azienda di cyber AI, ha annunciato che i clienti che utilizzano la sua soluzione per la sicurezza della posta elettronica basata sull'IA, Antigena Email, sono raddoppiati dal gennaio 2020 a oggi, e che il numero di richieste di prova della

soluzione è quadruplicato dall'inizio del lockdown. In particolare, nel mese di aprile, Darktrace ha rilevato come il 60% di tutti gli attacchi avanzati di spear-phishing bloccati da Antigena Email fossero correlati al COVID-19 o cercassero di ingannare i dipendenti facendo riferimento al lavoro da remoto. Chi attacca, infatti, sfrutta in modo sempre più consistente le preoccupazioni legate alla pandemia, per convincere le persone ad aprire i messaggi e cliccare su collegamenti dannosi; un fenomeno che Darktrace ha denominato "fearware" e che ha sfruttato oltre 48.000 domini di posta elettronica appositamente creati e correlati al coronavirus per

bypassare i filtri antispam standard.

La capacità di Antigena Email di distinguere le e-mail dannose dalle comunicazioni aziendali legittime, e impedire alle prime di raggiungere la casella della posta in arrivo del dipendente, si sta rivelando fondamentale, ha osservato l'azienda.

Alimentata dalla cyber AI, la tecnologia opera sfruttando la comprensione attività considerate normali per gli ambienti di posta elettronica aziendale e per i loro singoli utenti.

In questo modo è in grado di rilevare nuove minacce e attacchi mirati in arrivo che gli strumenti tradizionali lasciano passare, come lo spoofing del dominio,

il takeover degli account della catena di approvvigionamento o i tentativi di imitazione.

Darktrace ha bloccato numerose istanze di "fe-ware" indirizzate ai propri clienti. Ad esempio, presso il famoso studio di produzione Bunim/Murray a Los Angeles, Antigena Email ha identificato diverse e-mail di phishing che fingevano di fornire aggiornamenti sul COVID-19 ai dipendenti da parte dell'azienda.

ZSCALER SI ESPANDE E MIGLIORA LA SECURITY NEL CLOUD

Con l'annuncio dell'acquisizione di Cloudneeti la società estende al cloud pubblico il portfolio per la protezione della piattaforma Zscaler Cloud Security

di Giuseppe Saccardi

Zscaler, società attiva nel campo della cloud security, ha annunciato l'intenzione di acquisire Cloudneeti, una società che sviluppa soluzioni di Cloud Security Posture Management (CSPM).

Con l'acquisizione, Zscaler fornirà ai clienti una protezione dei dati all'interno della piattaforma Zscaler Cloud Security.

Il portfolio di Cloudneeti comprende soluzioni per prevenire e porre rimedio alle configurazioni errate negli ambienti SaaS, IaaS e PaaS, configurazioni errate che sono una delle principali cause di violazioni dei dati e di mancanza di conformità nelle applicazioni cloud.

«Sia che siano causate da applicazioni SaaS configurate in modo errato o da uno sviluppatore che ha accidentalmente sbagliato la configurazione di una nuova applicazione nel cloud pubblico, queste lacune nella protezione dei dati, che sono alla base di alcune delle più grandi violazioni della storia, si potranno prevenire. Sono orgoglioso quindi di dare il benvenuto al team Cloudneeti nella famiglia Zscaler», ha dichiarato Jay Chaudhry, Presidente e CEO di Zscaler.

«Se queste e-mail avessero raggiunto l'utente, uno dei nostri dipendenti, anche se in buona fede, avrebbe potuto cliccare sul collegamento malevolo nel tentativo di ottenere informazioni aggiornate e affidabili, senza capire che così avrebbe introdotto malware nel nostro ambiente», ha spiegato Gabe Cortina, CTO di Bunim/Murray. ❖



Il servizio fornito in modalità cloud

Zscaler Cloud Security Platform è una soluzione creata appositamente, ha spiegato la società, per aiutare le aziende a garantire sicurezza avanzata e aiutare nel percorso di trasformazione digitale.

Al portfolio Zscaler per la protezione dei dati per le applicazioni SaaS con CASB, Cloudneeti aggiunge la protezione dei dati dei carichi di lavoro del cloud pubblico e espande il portfolio di protezione dei dati di Zscaler con una serie di funzionalità che comprendono:

- Protezione dei dati e prevenzione dell'esposizione: le policy di protezione dei dati si applicano su qualsiasi tipo di sede, utenti e applicazioni in conformità con le normative come il GDPR.
- Conformità unificata: un'unica piattaforma fornisce visibilità della conformità e neutralizzazione delle violazioni in applicazioni SaaS come Microsoft Office 365 e a fornitori di servizi cloud, tra cui Amazon Web Services e Microsoft Azure.
- Riduzione del rischio: misure correttive automatiche assicurano che le applicazioni in cloud non siano vulnerabili alle minacce esterne seguendo le policy aziendali e di settore.

In pratica, le funzionalità di Cloudneeti rafforzeranno quelle di protezione dei dati di Zscaler Internet Access (ZIA) e della soluzione Cloud Access Security Broker (CASB) out-of-band di Zscaler.

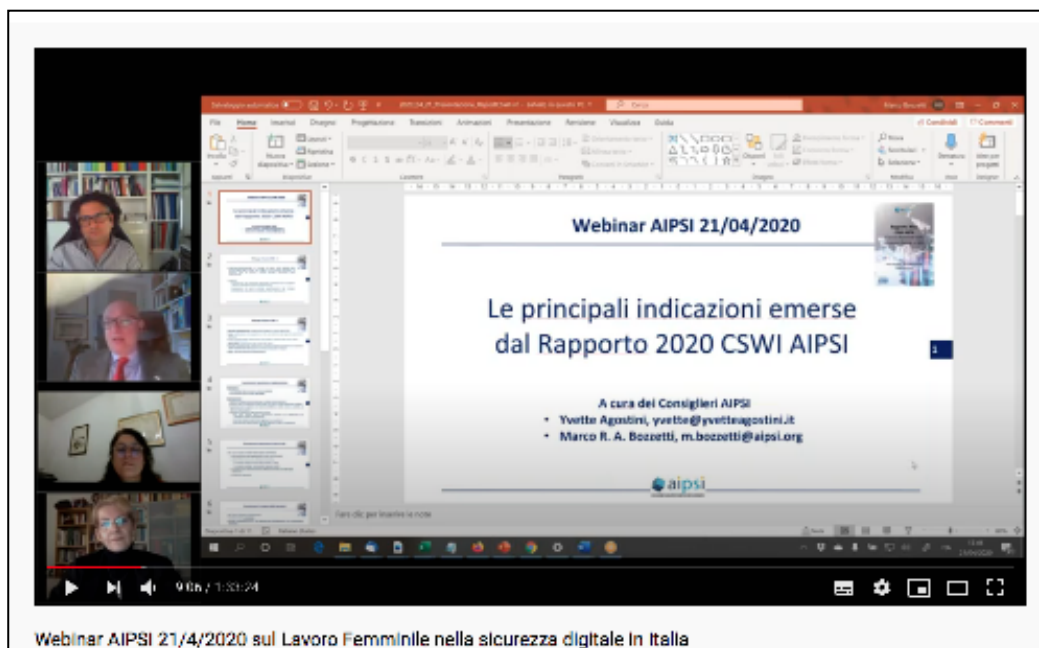
A livello finanziario e di enti di autorizzazione si prevede che l'operazione si concluderà entro la fine del terzo trimestre fiscale di Zscaler, subordinatamente al soddisfacimento delle consuete condizioni di closing. ❖

IL LAVORO FEMMINILE NELLA SICUREZZA DIGITALE IN ITALIA

Considerazioni dal Rapporto 2020 CSWI e dalla Tavola Rotonda del 21/4/2020

di *Yvette Agostini*,
Consigliera AIPSI e responsabile CSWI
Marco R. A. Bozzetti,
Presidente AIPSI

AIPSI a metà 2018 ha attivato il Gruppo di Lavoro CSWI, Cyber Security Women Italy, riservato alle donne (socio AIPSI o non) che svolgono la loro attività lavorativa, in qualsiasi ruolo ed anche a tempo parziale, nell'ambito della sicurezza digitale. I principali obiettivi di CSWI includono la creazione di una community femminile di donne che si occupano nella loro attività lavorativa di sicurezza digitale e la realizzazione di servizi orientati specificamente allo



Guarda il video del webinar AIPSI su YouTube



- AIPSI, Associazione Italiana Professionisti Sicurezza Informatica (<https://www.aipsi.org/>), è una libera associazione apolitica e a-religiosa, capitolo italiano della mondiale ISSA (<https://www.issa.org/>). L'obiettivo principale di AIPSI è aiutare i propri Soci nella loro crescita professionale, con la costituzione di una comunità interoperativa di professionisti e con il continuo aggiornamento delle competenze, così da consentire lo sviluppo della loro carriera professionale. Tali obiettivo è perseguito con la fornitura di servizi sia lato ISSA sia lato AIPSI: tra questi la rivista mensile ISSA Journal, le indagini in Italia CSWI ed OAD, i convegni ed i webinar, i position paper AIPSI, il supporto alle certificazioni eCF, etc.



sviluppo professionale delle donne che operano in questo settore. La guida di CSWI è stata assunta dall'ing. Yvette Agostini, Consigliera di AIPSI.

Il primo servizio realizzato è stata l'indagine sulla attuale situazione in Italia del lavoro femminile nella sicurezza digitale. La realizzazione dell'indagine è stata lunga, è durata in pratica l'intero anno 2019, per diversi motivi, tra i quali l'adesione a CSWI di varie professioniste, la messa a punto dei contenuti del questionario da effettuarsi on line, la ragionevole assicurazione che le rispondenti fossero veramente solo donne, e che le risposte al questionario fossero anonime.

Dopo vari incontri e discussioni all'interno del Gruppo di Lavoro CSWI, il questionario è risultato di 24 domande con risposte predefinite a scelta univoca o multipla, ed alcune a risposta aperta, senza richiesta di informazioni personale e/o identificative della compilatrice e della sua azienda/ente di appartenenza. Il tempo medio per la sua compilazione era tra i 10 e 15 minuti. Il questionario è stato posto on line nell'ambito del dominio aipsi.org utilizzando l'applicazione open source LimeSurvey. Per garantire, almeno in buona approssimazione, che le rispondenti fossero solo donne, l'indirizzo web del questionario non è stato reso pubblico, ma inviato in e-mail da AIPSI

- Il termine "sicurezza digitale" è usato per includere sia la sicurezza informatica che delle telecomunicazioni. In italiano il termine concettualmente equivalente è sicurezza ICT (ma non tutti conoscono l'acronimo ICT, Information and Communication Technology), in inglese Cyber Security

alle donne dell'associazione, del gruppo di lavoro CSWI, a quelle registrate al sito web dell'associazione e alla sua newsletter. A queste si sono aggiunte le donne che, a seguito della campagna di promozione per compilare il questionario, avevano chiesto via e-mail di avere l'indirizzo del questionario. Per ulteriormente garantire l'anonimato delle risposte, il sistema on line non registrava l'indirizzo IP del browser della rispondente e sulla banca dati delle risposte non veniva registrata la data e l'ora di inizio e fine compilazione. Essendo l'indagine anonima e liberamente fruibile dalle donne che hanno ricevuto l'indirizzo web del questionario, essa non ha alcun valore strettamente statistico, ma fornisce interessanti indicazioni sulle differenze di genere nel verticale settore della sicurezza digitale in Italia.

Le risposte al questionario sono state elaborate da Agostini e Bozzetti, che hanno pubblicato il Rapporto 2020 CSWI, costituito da 39 pagine formato A4 e gratuitamente scaricabile da <https://www.aipsi.org/aree-tematiche/cswi-cyber-security-women-s-italy/rapporto-2020-cswi-aipsi.html>

Nel complesso le rispondenti sono state 247, la maggior parte delle quali, 49,1%, giovani con età compresa tra i 25 e i 34 anni, e con un elevato grado di preparazione: il 43,9% ha conseguito una laurea magistrale, e di queste il 55,3% del settore tecnico-scientifico, il 26,5% ha conseguito un dottorato o un master ed il 73,1% ha conseguito certificazioni professionali specifiche sull'ICT.

Le rispondenti sono in maggioranza giovani non solo anagraficamente, ma anche temporalmente, ossia da quanto si occupano per lavoro di cybersecurity: il 60% arriva al massimo a 5 anni di attività.

Per la maggior parte delle rispondenti, 52,6%, la conciliazione dei tempi del lavoro con quelli personali/famigliari presenta delle difficoltà anche se l'essere donna nell'ambito di questa attività lavorativa è indifferente per il 51,9% e presenta un vantaggio per il 9,3%.

La differenza di genere si evidenzia a livello retributivo anche in questo settore: a parità di ruolo, responsabilità, competenza ed anzianità il 38% dichiara di essere pagata meno degli uomini

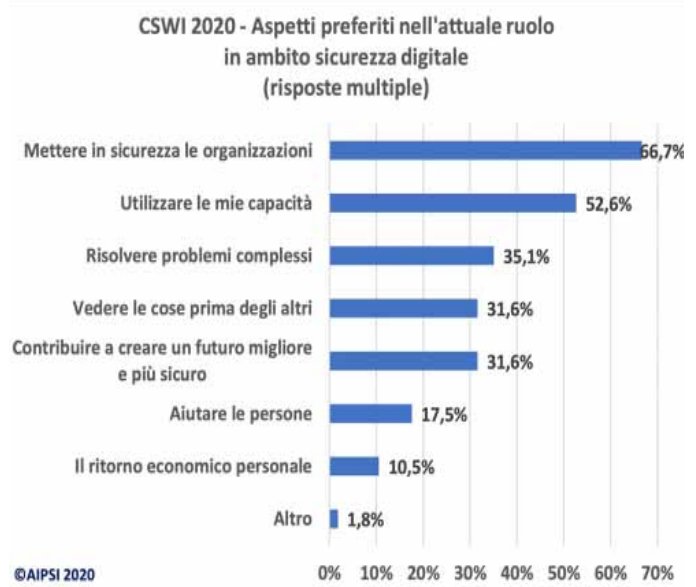
Ulteriori difficoltà evidenziate nell'indagine includono l'effettivo tempo di lavoro necessario/richiesto, sempre assai superiore alle 8 ore contrattuali, la frequente mancanza di supporto e collaborazione da parte dei colleghi/dal team di lavoro, la non disponibilità di efficaci strumenti informatici per il supporto e l'automazione di parti del proprio lavoro.

Gli aspetti positivi evidenziati dalle rispondenti nel lavorare nell'ambito della sicurezza digitale includono l'interdisciplinarietà della materia, le varie opportunità e le varie sfide che porta, e soprattutto il poter utilizzare le proprie capacità. La figura sottostante, presa dal Rapporto 2020 CSWI, evidenzia quali sono gli aspetti preferiti dalle rispondenti nel loro attuale ruolo nell'ambito della sicurezza digitale. Interessante evidenziare come il ritorno economico sia in pratica all'ultimo posto.

I principali desiderata nel prossimo futuro professionale delle rispondenti include il poter acquisire maggiori competenze, il poter operare in posizioni di maggior responsabilità e potere e, soprattutto, il poter lavorare in aziende che investono e valorizzano le proprie risorse umane.

Nel corso di un webinar tenuto il 21/4/2020, dopo aver presentato questi dati, è stato assai significativo poterli commentare e discutere in un tavolo rotondo cui hanno partecipato alcune donne dal ruolo e responsabilità assai significative nel campo della sicurezza digitale:

- dott.a **Marella Folgori**, Italy, Russia & CIS Sales Leader Security & Manageability Oracle
- dott.a **Adriana Franca**, Country Manager digiTree Italia
- dott.a **Paola Generali**, Presidente Assintel, Consigliera della Camera di Commercio MI, MB e LO, Managing Director GetSolution



- prof.a **Donatella Sciuto**, Prorettore Vicario del Politecnico di Milano, Professore ordinario di Architettura dei calcolatori e sistemi operativi

- avv.a **Carla Secchieri**, Consigliera CNF, VP FiiF-CNF, Coordinatrice corso DPO CNF-Ordine Ingegneri
Per impegni improrogabili all'ultimo momento non ha potuto partecipare la dott.a Nunzia Ciardi, Direttore Servizio Polizia Postale e delle Comunicazioni.

Quanto emerso dalla tavola rotonda è sintetizzabile nei seguenti punti, sui quali tutte le partecipanti hanno concordato:

- le differenze di genere evidenziate nel Rapporto sono comuni alla stragrande maggioranza dei diversi lavori effettuati da donne: differenze soprattutto a livello retributivo
- sono ancora assai poche le donne che in Italia si occupano di sicurezza digitale, ed ancora meno quelle che se ne occupano da un punto strettamente tecnico. Questo è dovuto principalmente a pregiudizi e mentalità famigliari, che scoraggiano una giovane dall'intraprendere una carriera tecnica-manageriale nella sicurezza digitale: è un mestiere da uomini, le donne è meglio che facciano le insegnanti, gli avvocati, le dottoresse in medicina; e, se proprio vogliono dedicarsi alla sicurezza, la compliance è considerata più adatta.
- Al contrario le donne che operano nell'ambito della sicurezza digitale sono, nella maggior parte dei casi sia a livello aziende della domanda che a quello dell'offerta, estremamente preparate e qualificate: risultano essere, rispetto ai colleghi uomini più pragmatiche e sanno meglio bilanciare gli aspetti

tecnici/digitali con quelli umani

- In ambito internazionale la situazione è diversa da quella italiana, per cultura, modelli e logiche nel lavoro. Anche a livello scolastico ed accademico l'Italia è in ritardo su questi temi, ma alcuni recenti ed innovativi corsi universitari riescono a ridurre tale gap, anche di interesse, e sono frequentati praticamente alla pari da uomini e da donne
- Il bilanciamento tra attività lavorativa e personale/famigliare è critico per le donne, soprattutto se hanno famiglia. La repentina necessità di smart working causata dalla pandemia del Covid-19 fornisce sicuramente uno strumento di ausilio e facilitatore, che richiede una quotidiana autoregolamentazione
- È necessaria comunque una riforma anche legislativa per realmente equiparare il lavoro femminile con quello maschile, in primis a livello retributivo
- Tutte le partecipanti alla tavola rotonda, coi loro diversi ed impegnativi ruoli, utilizzano fortemente gli strumenti informatici per far fronte ai loro impressionanti carichi di lavoro.

In conclusione, la sicurezza digitale è sempre più una grande opportunità per le donne, che la devono cogliere fin dagli inizi della loro carriera sfruttando al meglio le innovazioni tecnologiche e superando le ancora esistenti barriere culturali ed informative sulla digitalizzazione e la sua sicurezza. Ed in tale ottica si muove e si muoverà sempre più AIPSI, in collaborazione anche con altre associazioni ed enti pubblici. ❖

È disponibile il nuovo libro
SMART & DIGITAL TRANSFORMATION

A nighttime cityscape featuring a prominent skyscraper with a blue-lit spire. The scene is overlaid with a purple-toned network of white lines and dots, suggesting digital connectivity. A white-bordered box is centered over the image, containing the book's title and a subtitle.

SMART & DIGITAL TRANSFORMATION

Aziende, ambienti produttivi e città sono sempre più
Smart, ma si deve garantire flessibilità, always-on,
sicurezza e accesso al multicloud

Il libro è acquistabile al prezzo di 30 euro (IVA inclusa) richiedendolo a
info@reportec.it - tel 02 36580441 - fax 02 36580444