SECURITY & BUSINESS

n. 55

CYBER ATTACK
EMOTET E VALAK MINANO LA SECURITY IN ITALIA

pag. 04

IN QUESTO NUMERO:

CYBER ATTACK

pag. 04
Emotet e Valak minano la security in Italia

pag. 06
Conosci il livello di sicurezza della tua azienda?

SOLUZIONI

pag. 08
- ArcSight SOAR: sicurezza più automatizzata ed efficiente

pag. 11
- Le best practice per la cyber security le suggerisce CyberArk

pag. 13
- Pagamenti elettronici conformi PSP2 con la biometria Nuance

pag. 15
- Stormshield Endpoint Security Evolution protegge le Workstation

pag. 17
- Navigare in sicurezza con ESET Internet Security

STRATEGIE&MERCATI

pag. 19
- ICOS potenzia la divisione Cyber security

pag. 19
- Andrea Negroni Country leader cybersecurity di Cisco per l'Italia

Reportec

OAD 2020

L'iniziativa OAD, Osservatorio Attacchi Digitali in Italia, con il 2020 è alla 12° edizione, con 12 anni consecutivi di indagini sugli attacchi digitali intenzionali ad aziende ed enti pubblici in Italia.
OAD è l'unica iniziativa in Italia per l'analisi sugli attacchi, realizzata tramite una indagine anonima con un questionario compilabile on line, indirizzata a tutte le aziende e alle Pubbliche Amministrazioni di ogni settore merceologico e dimensione. OAD collabora con la Polizia Postale e delle Comunicazioni, che fornisce significativi dati sugli attacchi digitali che costituiscono crimini informatici.
Obiettivo principale di OAD è fornire reali e concrete indicazioni sugli attacchi ai sistemi informatici che possano essere di riferimento nazionale, autorevole e indipendente, per la sicurezza ICT in Italia e per l'analisi dei rischi ICT. La disponibilità di dati "locali all'Italia" sugli attacchi digitali intenzionali rilevati, sulla tipologia e sull'ampiezza del fenomeno è fondamentale anche per le organizzazioni di piccole e piccolissime dimensioni per valutare i possibili rischi e attivare le misure più idonee di prevenzione e protezione, così come richiesto da numerose normative nazionali ed internazionali, non ultimo il GDPR, il regolamento europeo sulla privacy. OAD, con la sua indagine e con lo stretto supporto di AIPSI, Associazione Italiana Professionisti Sicurezza Digitale (Capitolo italiano della mondiale ISSA), intende inoltre contribuire alla sensibilizzazione e alla consapevolezza, in Italia, sulla sicurezza digitale del personale a tutti i livelli, dai decisori di vertice agli utenti. Quest'ultimo obiettivo è particolarmente importante per creare una più diffusa cultura in materia di sicurezza digitale, che va oltre il mondo tecnico-informatico e tocca anche i vertici dell'organizzazione e tutti coloro che decidono requisiti e budget della sicurezza digitale nei processi organizzativi delle proprie strutture.
Per la prima volta nell'edizione 2020, chi completa il questionario on line avrà anche in tempo reale una valutazione di sintesi di come le misure di sicurezza digitale indicate rispondano effettivamente alle esigenze di sicurezza digitale indicate per l'azienda/ente ed il suo sistema informatico: una macro valutazione qualitativa (e gratuita) del livello di sicurezza digitale del sistema informatico oggetto delle risposte fornite provevinel rispondere al questionario.
Per motivare il rispondente, a conclusione delle risposte fornite al questionario on line, oltre alla valutazione di cui sopra, è possibile scaricare gratuitamente il numero di maggio 2020 di ISSA Journal, la rivista mensile riservata ai soci AIPSI-ISSA, che tratta la crittografia quantistica, e l'intero volume "Information Security e Data Protection", pubblicato da Reportec, che è anche Publisher e Media Partner per OAD.
Il Rapporto finale di OAD 2020 è previsto per fine novembre 2020, e sarà scaricabile gratuitamente da parte di tutti gli interessati. Più compilazioni del questionario si avranno, provenienti dai vari settori merceologici e dalle Pubbliche Amministrazioni Centrali e Locali, più analitico, dettagliato, accurato e autorevole potrà essere il rapporto finale.

Si prega pertanto il lettore di questa nota di compilare, o di far compilare dai suoi tecnici, il questionario on line disponibile alla pagina: https://www.oadweb.it/limesurvey2020/index.php/574592?lang=it

OAD
Osservatorio
Attacchi Digitali
in Italia

Security & Business 55
settembre-ottobre 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

GLI SCENARI D'ATTACCO, LE SOLUZIONI E LE DINAMICHE DI MERCATO

La novità principale di questo numero di Security & Business riguarda una nuova rubrica che ospiterà sia articoli sia brevi news, destinate presentare dinamiche e strategie di mercato. Sono principalmente informazioni indirizzate agli addetti ai lavori. Importanti in un mercato critico, quale quello della sicurezza.

La rubrica Cyber Attack scende nel dettaglio delle minacce in Italia e nel resto del mondo, relativamente a malware "mutante". Non stiamo parlando di una nuova serie televisiva, il che è un peccato, perché se si riuscisse a replicare gli ascolti di "Io Robot", oggi che le piattaforme in streaming sono così popolari si avrebbe una forte leva per accrescere la cultura della sicurezza. Un comportamento più accorto disarmerebbe molti malintenzionati e ridurrebbe enormemente i danni.

Una piuttosto approfondita analisi sulle minacce relative ai malware Valak ed Emotec, realizzata da CheckPoint Software Technology, mostra alcune delle dinamiche adottate dai cybercriminali nella gestione del loro "business", per esempio sul modo di riciclare gli strumenti di attacco.

Ma in tema di attacchi, in particolare attacchi che hanno colpito aziende italiane, uno strumento fondamentale è il rapporto OAD, che non solo è ''unico basato sui dati italiani, con una lunga storia, m anche perché da quest'anno al termine della compilazione del rapido questionario si ottiene immediatamente un indice dello stato attuale della propria sicurezza aziendale.

La rubrica sulle soluzioni, infine, presenta alcune delle più recenti tecnologie per aumentare la protezione dei dati e delle infrastrutture delle impoprese.

EMOTET E VALAK MINANO LA SECURITY IN ITALIA

Il nuovo Global Threat Index mensile, emesso da Check Point Software Technologies mostra le minacce del momento

di Gaetano Di Blasio

La "classifica Top 10" degli attacchi a settembre è, per la prima volta, guidata da una variante dell' info-stealer di Valak, secondo il Global Threat Index di Check Point Software Technologies.

Tale variante si posiziona, però, solo quarta in Italia, dove permane al primo posto il trojan Emotet per il terzo mese consecutivo.

Ciononostante il malware Valak, secondo i ricercatori, mostra comunque un importante aumento degli attacchi piazzandosi al I nono posto fra i malware più diffusi nel mondo e al quarto in Italia, pur se con una quota bassa (3%) dovuta a una predominanza di Emotet .

Valak è una minaccia molto sofisticata, ci dicono gli esperti di Check Point spiegando che genera nuove varianti con cambiamenti considerevoli nel tempo (è stato visto per la prima volta a fine 2019). Di recente alcune derivazioni hanno permesso di trafugare informazioni sensibili dai sistemi di posta elettronica di Microsoft Exchange, nonché credenziali degli utenti e i certificati di dominio. In settembre Valak è stato utilizzato molto campagne malevole via spam, contenenti file .doc dannosi.

Altre rivelazioni riguardano l'impatto di Emotet, quantificabile in un effetto sul 14% delle organizzazioni a livello globale.

Il il trojan Qbot, invece, apparso nella Top10 la prima volta ad settembre, è stato molto sfruttato anche a settembre, passando dal decimo al sesto posto.

Maya Horowitz, Director, Threat Intelligence & Research, Products di Check Point ha commentato:« Queste nuove campagne di diffusione di Valak sono un altro esempio di come gli aggressori cercano di massimizzare i loro investimenti in forme consolidate e comprovate di malware. Insieme alle versioni aggiornate di Qbot, emerse in settembre, Valak ha lo scopo di consentire il furto di dati e credenziali su larga scala sia a organizzazioni che privati.

Le aziende dovrebbero cercare di implementare soluzioni anti-malware in grado di impedire che tali contenuti raggiungano gli utenti finali e consigliare ai propri dipendenti di essere prudenti nell'aprire le e-mail, anche quando sembrano provenire da una fonte affidabile».

Inoltre, aggiunge Horowitz: «Queste nuove campagne di Valak sono un altro esempio di come i cyber criminali cerchino di ottenere il massimo dai i loro investimenti sfruttando tecnologie consolidate e di dimostrata efficacia».

Con le versioni aggiornate di Qbot, affiorate in settembre, Valak è usato per tentare il furto di dati e credenziali digitali su larga scala mirando sia ad aziende sia a privati.

I 3 malware più diffusi di settembre

I 3 malware più diffusi di settembre sono stati: Emotet; Trickbot; Dridex.

Emotet è un avanzato, autopropagante e modulare, che è usato anche per distribuire altre minacce, infatti utilizza molteplici metodi per mantenere la stabilità e le tecniche di evasione per evitare il rilevamento. Si diffonde anche attraverso campagne phishing con mail contenenti allegati o link dannosi.

Trickbot consiste in banking trojan che viene aggiornato costantemente con nuove funzioni. Questi fattori lo rendono un malware flessibile e personalizzabile che può essere diffuso tramite vari tipi di campagne.

Dridex è anch'esso- banking trojan il quale è specializzato per colpire la di piattaforma Windows. È usato attraverso campagne spam e kit di exploiter, intercettare e reindirizzare le credenziali bancarie a un server controllato dagli aggressori. Dridex contatta un server remoto, invia informazioni sul sistema infetto e può anche scaricare ed eseguire moduli aggiuntivi per il controllo da remoto.

Le vulnerabilità più sfruttate in settembre:

A settembre "MVPower DVR Remote Code Execution" è stata la più comune vulnerabilità sfruttata, con un impatto sul 46% delle organizzazioni a livello globale, seguita da "Dasan GPON Router Authentication Bypass" che ha avuto un impatto sul 42%. Poi, "OpenSSL TLS DTLS Heartbeat Information Disclosure (CVE-2014-0160; CVE-2014-0346" al terzo posto, con il 36%.

I tre malware mobile più diffusi di settembre

Anche a settembre xHelper è il malware mobile più diffuso, seguito da Xafecopy e Hiddad.

xHelper - un'applicazione Android dannosa, individuata a marzo 2019, utilizzata per scaricare altre app dannose e visualizzare pubblicità. È capace di nascondersi dall'utente e dai programmi antivirus mobile, e si reinstalla se l'utente la disinstalla.

Xafekopy - trojan camuffato da app utili come Battery Master. Carica segretamente codice dannoso sul dispositivo; una volta attivata l'app, clicca sulle pagine web con la fatturazione del Wireless Application Protocol (WAP) - una forma di pagamento mobile che addebita i costi direttamente sulla bolletta del cellulare dell'utente.

Hiddad - malware Android che riconfeziona app legali e poi le consegna a uno store di terze parti. La sua funzione principale è visualizzare annunci, ma è anche in grado di accedere ai dati chiave di sicurezza, integrati nel sistema operativo, consentendo all'aggressore di ottenere dati sensibili dell'utente.

La ThreatCloud Map e il Global Threat Impact Index di Check Point si avvalgono dell'intelligence ThreatCloud : la più grande organizzazione contro i cybercriminali che fornisce dati sulle minacce e sull'andamento degli attacchi, attraverso una rete globale di sensori delle minacce. Il database di ThreatCloud ispeziona oltre 2,5 miliardi di siti web e 500 milioni di file, e ogni giorno identifica più di 250 milioni di attività malware.

La lista completa delle 10 famiglie di malware più attive nel mese di settembre è disponibile sul blog di Check Point. ❖

CONOSCI IL LIVELLO DI SICUREZZA DELLA TUA AZIENDA?

Una macro valutazione gratuita del livello di sicurezza digitale del tuo sistema informatico, compilando l'anonimo questionario OAD 2020

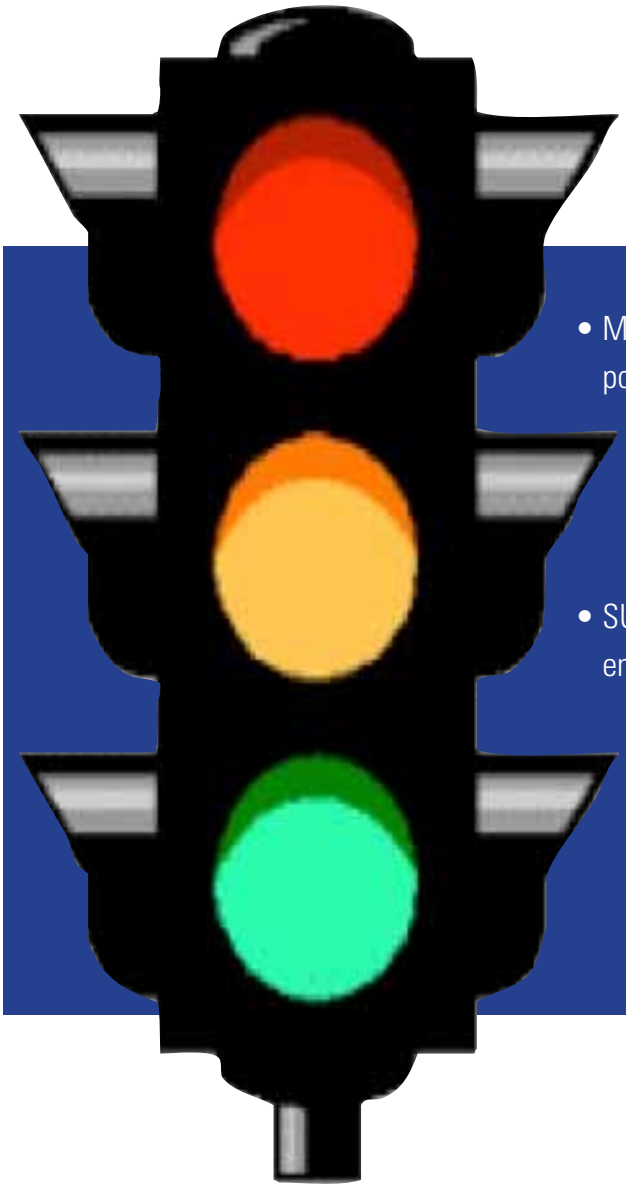
di Marco Bozzetti

Il Questionario 2020 OAD, Osservatorio Attacchi Digitali in Italia, **totalmente anonimo**, è compilabile on line all'indirizzo: https://www.oadweb.it/limesurvey2020/index.php/574592?lang=it

L'indagine OAD, quest'anno al 12° anno consecutivo di indagini, è l'unica in Italia ad essere effettuata on line, liberamente rivolta ad aziende di ogni dimensione e settore merceologico, oltre che agli enti pubblici. L'elaborazione dei dati raccolti porta alla pubblicazione del rapporto finale annuale: il piano di lavoro con tutte le scadenze previste per il 2020 è alla pagina https://www.oadweb.it/it/oad-2020.html. Tutti i rapporti annuali e le relative presentazioni, articoli e filmati sull'argomento sono scaricabili/visibili da https://www.oadweb.it/it/

Rispondere al questionario, oltre ad un veloce ma preciso ripasso-aggiornamento sui possibili attacchi, e sulle misure di sicurezza digitale, consente di ottenere una **valutazione qualitativa sul livello di sicurezza digitale** del sistema informatico oggetto delle risposte; tale valutazione è contestualizzata alla necessità di sicurezza digitale dell'azienda/ente rispondente e del suo sistema informatico, necessità derivata dalle risposte selezionate. Sempre a conclusione della compilazione, potrà scaricare gratuitamente in formato pdf il numero di maggio 2020 di **ISSA Journal** sulla crittografia quantistica (la rivista mensile riservata ai Soci AIPSI) e la seconda edizione 2019 del volume di G. Saccardi, G. Di Blasio, R. Florio "**Information Security e Data Protection 2019**", pubblicato per i tipi di Reportec.

La valutazione qualitativa del livello di sicurezza del sistema informatico considerato nelle risposte selezionate da chi compila il questionario si basa sul "peso" attribuito ad ogni risposta selezionabile del questionario. È attribuito un peso alle risposte sulle misure tecniche ed organizzative: più è alto il valore del peso, più elevato è il livello della misura di sicurezza digitale. È attribuito un peso anche al tipo di azienda/ente ed alle sue primarie caratteristiche per individuare qualitativamente la necessità di sicurezza digitale dell'azienda/ente in funzione delle sue attività e del suo business. La differenza tra il valore complessivo della necessità di sicurezza digitale ed il valore complessivo delle misure di sicurezza tecniche ed organizzative in atto costituisce l'indice di sicurezza digitale che, per gamma (range) di valori predefiniti fornisce la valutazione qualitativa:



- MOLTO CRITICO: urgono significativi interventi di potenziamento della sicurezza a livello tecnico ed organizzativo
- INSUFFICIENTE: urgono interventi di miglioramento della sicurezza a livello tecnico ed organizzativo
- SUFFICIENTE: rispetto alle esigenze dell'azienda/ente, le misure di sicurezza in atto sono sufficienti, ma sarebbe opportuno potenziarle
- BUONO: rispetto alle esigenze dell'azienda/ente, le misure di sicurezza in atto sono ad alto livello, ma è opportuno mantenerle a questi livelli con sistematici interventi sia tecnici sia organizzativi.

Tale valutazione appare in automatico al completamento del questionario, evidenziata sul browser di chi compila da un semaforo.

Si invitano caldamente tutti i lettori a compilare, o a far compilare dai loro informatici, il Questionario 2020 OAD, e di "passare parola" per questa compilazione ai loro interlocutori. Più risposte si avranno, soprattutto distribuite per i diversi settori merceologici, più autorevole e rappresentativo della realtà italiano sugli attacchi digitali potrà essere il rapporto finale 2020 OAD. ❖

ARCSIGHT SOAR: SICUREZZA PIÙ AUTOMATIZZATA ED EFFICIENTE

L'ultimo tassello della famiglia ArcSight permette di automatizzare i compiti ripetitivi e di orchestrare in modo ottimizzato la gestione degli incidenti e le attività di risposta

*di **Riccardo Florio***

Micro Focus ArcSight SOAR è il componente più recente della famiglia di soluzioni software Micro Focus ArcSight. SI tratta, come suggerisce l'acronimo, di una piattaforma di Security Orchestration, Automation and Response che aiuta le aziende e migliorare l'efficienza di risposta agli attacchi grazie alla sua capacità di combinare automazione, gestione degli incidenti e capacità di orchestrazione.

«ArcSight SOAR aiuta i team di sicurezza a definire le priorità di intervento e a predisporre attività standardizzate di riposta agli incidenti - spiega Pierpaolo Alì, Director Southern Europe Security, Risk & Governance di Micro Focus -. Le sue funzionalità di gestione centralizzata e di automazione di tutti i compiti ripetitivi aumentano il livello di protezione, accelerano la capacità di risposta e ottimizzano il tempo prezioso dei professionisti della sicurezza che operano all'interno dei SOC. L'integrazione nativa con le altre tecnologie Micro Focus concorre a realizzare un modello di sicurezza Zero Trust».

Micro Focus ArcSight SOAR

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

Ottimizzare la Security Orchestration

In sintesi, le funzioni fondamentali svolte da ArcSight SOAR sono: automazione di processo, controllo centralizzato delle Security Operation da un unico pannello di comando, capacità di indagine e risposta in modo collaborativo, raccolta e misura di tutte le attività legate alla sicurezza.

ArcSight SOAR mette a disposizione un motore di automazione programmabile che si integra con oltre 120 diverse infrastrutture e strumenti di sicurezza, con la possibilità di interrogare i sistemi per individuare un attacco in corso e intraprendere azioni di blocco.

Attraverso un service desk unificato è possibile gestire tutti gli incidenti di sicurezza provenienti da SIEM, da altri service desk, da moduli Web, da applicazioni di terze parti e così via.

Inoltre, ArcSight SOAR registra ogni attività e inoltra tutti i dati alla piattaforma SIEM. Attraverso l'analisi di tutti gli eventi vengono realizzate metriche, prodotti report dettagliati e costruita un Timeline che favorisce le operazioni di analisi, audit e pianificazione.

Difesa integrata con le tecnologie SOAR, SIEM e UEBA di Micro Focus

ArcSight SOAR è nativamente disponibile all'interno della soluzione ArcSight ESM per la gestione di informazioni ed eventi di sicurezza (SIEM). Attraverso l'ulteriore integrazione con la tecnologia Interset per l'analisi del comportamento (UEBA, acronimo di User and Entity Behaviour Analytics) si ottiene il massimo livello di efficienza operativa e di sicurezza all'interno del Security Operation Center (SOC).

Vediamo tre esempi di situazioni in cui queste tre tecnologie operano sinergicamente con successo.

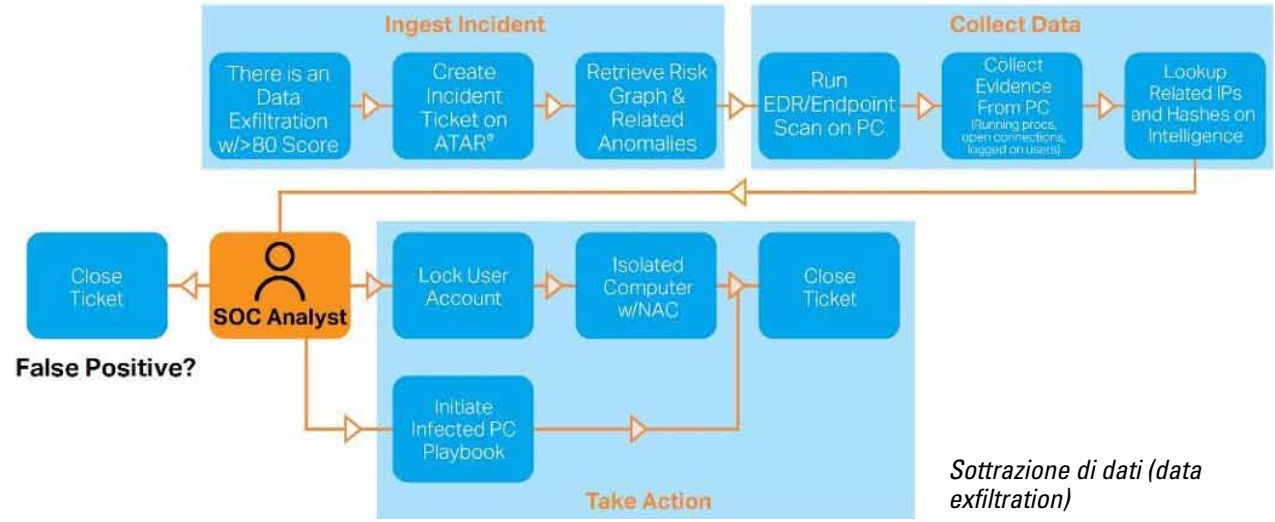
- **Assegnazione della priorità a un evento di sicurezza**. L'uso combinato di queste tre tecnologie permette di rispondere all'esigenza di ridurre il carico dovuto alle migliaia di avvisi di sicurezza che le imprese ricevono ogni giorno. ArcSight SOAR integrato con Micro Focus ArcSight ESM e Interset permette di analizzare gli allarmi e stabilire la priorità con cui gestirli. Il SIEM rileva gli eventi di sicurezza e genera un allarme che crea automaticamente un ticket. Interset elabora la situazione e fornisce un corrispondente indice di rischio e passa il compito a SOAR che, in base al valore dell'indice di rischio, assegna all'evento un livello di priorità con cui gestire l'attività di risposta.

Assegnazione automatica di priorità agli eventi di sicurezza

Compromissione di un account

- **Compromissione di un account.** Nel caso in cui si verifichi la compromissione di un account è essenziale che sia il rilevamento sia le azioni di risposta avvengano nel tempo più rapido possibile. ArcSight SOAR può raccogliere la segnalazione di un'anomalia da Interset e creare un ticket di incidente sul suo Service Desk di gestione degli incidenti. Sfruttando le sue capacità di integrazione, orchestrazione e automazione SOAR indaga e accerta la situazione (per esempio recuperando le attività di login dell'utente nelle ultime 48 ore) ed effettua le azioni necessarie per evitare la compromissione quali il blocco temporaneo dell'account e l'invio di una nuova password.

- **Data Exfiltration.** Identificare le situazioni in cui un malware o un cyber criminale stanno effettuano un trasferimento di dati non autorizzato non è semplice. Richiede la capacità di differenziare il flusso di traffico anomalo da quello normale trasmesso attraverso la rete. Utilizzando tecnologie di machine learning non supervisionato Micro Focus Interset rileva comportamenti inusuali che possono indicare un tentativo di Data Exfiltration. Informa, quindi, ArcSight SOAR che provvede a collegarsi ai pc sospetti, bloccare l'account dell'utente, raccogliere prove e isolare automaticamente la macchina dalla rete. ❖



Sottrazione di dati (data exfiltration)

LE BEST PRACTICE PER LA CYBER SECURITY LE SUGGERISCE CYBERARK

Paolo Lossa, Country Sales Manager di CyberArk Italia, ha messo in evidenza i cinque punti critici della cyber security nell'era del Covid e dello smart working

*di **Giuseppe Saccardi***

Ci si sta avviando alla fine del 2020, un anno di certo difficile per le aziende, che hanno dovuto ricorrere allo smart working e così facendo a dover rispondere ai problemi intrinsechi nel lavoro da remoto, soprattutto nel caso di utenti privilegiati i cui dati sono tra i più ambiti dai criminali cibernetici.

E' questo anche il mese di ottobre, il mese della Cyber Security Awareness, iniziativa oggi più che mai necessaria.

La crisi sanitaria, evidenzia poi Paolo Lossa, Country Sales Manager di CyberArk Italia, ha influenzato in modo significativo la nostra vita quotidiana e ci ha spinti a un utilizzo sempre più intenso delle tecnologie. È una combinazione di fattori che ha stimolato la creatività dei cyber criminali che hanno sviluppato nuove tecniche di attacco volte a catturare i nostri dati sensibili, la cui vendita sul dark web è molto redditizia.

Paolo Lossa, Country Sales Manager di CyberArk Italia

Ma cosa suggerisce Lossa? Innanzitutto che gli utenti devono conoscere i rischi informatici in cui potrebbero incorrere al fine di adottare l'approccio più appropriato per proteggere se stessi e i propri dispositivi. Molti aspetti della nostra vita quotidiana possono infatti diventare un punto di accesso per i cyber criminali, ma non tutti ne sono consapevoli.

Cinque i consigli suggeriti da Lossa per incrementare il livello di protezione. Vediamoli in sintesi:

Non fidarsi degli estranei è una regola imparata fin da piccoli, che vale anche nel mondo digitale. Infatti, non bisognerebbe mai aprire messaggi o cliccare su link ricevuti da persone che non si conoscono, che si tratti di e-mail, messaggi su Slack, Teams o Google Chat.

Monitorare la vostra salute va bene, farsi rubare i dati, no! Fitness tracker e orologi "intelligenti" hanno guadagnato popolarità nel corso degli anni perché sono un modo semplice per tenere sotto controllo la propria forma fisica, purtroppo però raccolgono molti

dati personali. Chi li utilizza – o sta pensando di acquistarne uno – deve quindi assicurarsi di sapere esattamente come vengono utilizzati, archiviati e protetti i dati personali dalle differenti aziende.

Non raccontarsi troppo sui social network. Se questi canali permettono di condividere le passioni e i bei momenti con le persone care, bisogna fare attenzione a non condividere informazioni personali che potrebbero essere utilizzate per determinare password e domande di sicurezza, indicare un luogo o prevedere il comportamento. Si tratta infatti di una miniera d'oro per i criminali che cercano la loro prossima vittima.

Proteggere lo smartphone. Le applicazioni sono parte integrante della nostra vita quotidiana. C'è qualcosa per tutto: fare shopping, prendere un appuntamento con un medico, conoscere il proprio saldo bancario ed effettuare bonifici, o sapere quando innaffiare le piante. I cellulari hanno assunto il ruolo di assistente personale, sia in ambito privato che professionale, ma non sono meno vulnerabili agli attacchi. Pertanto, è importante verificare a quali dati ogni applicazione ha accesso. Inoltre, migliori processi di autenticazione – come l'autenticazione a più fattori – aiutano a garantire che gli smartphone non vengano sfruttati dagli aggressori per rubare dati personali.

Proteggere l'Internet of Things. Nei prossimi dieci anni, ogni consumatore avrà almeno 10 dispositivi collegati e, se non sono sicuri, ognuno di essi rappresenterà un modo per rubare dati sensibili. I dispositivi IoT, come le smart TV e i contatori collegati, sono sicuramente utili, ma richiedono molte informazioni e connessioni per funzionare correttamente. Inoltre, diventano ogni giorno più intelligenti e si integrano tra loro, creando case e aziende completamente connesse. Per metterli in sicurezza e chiudere tutti gli accessi alla rete, è necessario fidarsi solo di produttori rinomati, applicare ogni patch di sicurezza disponibile e aggiornare le loro password di default.

La tecnologia, mette poi in guardia Lossa, sta entrando sempre più nelle nostre abitudini e gran parte delle nostre attività nel tempo libero, acquisti o operazioni amministrative ora includono la navigazione online. Pertanto, la protezione dei nostri dati personali e la prova della nostra identità saranno al centro di tutto ciò che facciamo fino al 2030. E, chissà, forse il nostro frigorifero connesso saprà più cose su di noi di noi stessi. ❖

PAGAMENTI ELETTRONICI CONFORMI PSP2 CON LA BIOMETRIA NUANCE

Crescono gli attacchi alle credenzialinel financial cyber crime, sale il bisogno dell'l'autenticazione forte. La direttiva in vigore da fine anno

di Gaetano Di Blasio

La nuova direttiva nota come PSP2 entrerà in vigore il 31 dicembre 2020 con l'obiettivo di promuovere l'innovazione digitale nel settore bancario e regolamentare i servizi di pagamento all'interno dell'Unione Europea. Un aspetto basilare su cui si fonda la direttiva è, ovviamente, l'intenzione di rafforzare la sicurezza dei pagamenti online, cresciuti vertiginosamente insieme con l'avanzare del commercio elettronico. A ciò si aggiunge la necessità di tutelare le parti coinvolte nell'aumento degli attacchi fraudolenti.

Preoccupa, in particolare il "financial cyber crime" indirizzato alla caccia di credenziali, codici personali e dati sensibili, nonché alla violazione dei sistemi bancari di privati e imprese.

Le statistiche hanno registrato quasi 5mila casi in Italia nel 2019. Gli analisti di Juniper Research hanno rilevato che i danni economici al mercato dei pagamenti digitali arrecati dalle frodi online supereranno i 200 miliardi di dollari tra il 2020 e il 2024. Una soluzione cui guarda con interesse il mercato è relativa all'uso dei parametri biometrici in fase sia di prevenzione sia di contrasto. Non a caso molti istituti di credito hanno scelto questo tipo di soluzioni. Nel settore opera da tempo Nuance Communications, specializzata nelle innovazioni di intelligenza artificiale conversazionale, investendo nel supporto alle le banche e alle organizzazioni di servizi finanziari nell'eseguire transazioni con il massimo livello di sicurezza attraverso tecnologie di autenticazione biometrica innovative e conformi alle nuove normative UE.

Le nuove direttive PSD2 e SCA

Secondo la direttiva che sarà in vigore a fine anno, in caso di pagamenti non autorizzati, il SPS ha la responsabilità di rimborsare immediatamente al cliente la somma corrispondente all'operazione. Per tutelare le parti coinvolte e limitare allo stesso tempo il rischio di frodi, la direttiva PSD2 ha introdotto la necessità di mettere in esercizio il processo di Strong Customer Authentication (l'autenticazione della persona che effettua il pagamento). Dal 31 dicembre dovrà includere almeno due dei tre elementi di base per 'autenticazione: conoscenza

Saverio Ricchiuto - Sales Director Enterprise Italia di Nuance

(PIN, password), possesso (carta di credito, token) e inerenza (biometria).

Per abilitare la SCA, parecchie aziende hanno scelto per l'invio di un codice o un PIN (OTP, One Time Password) tramite SMS.

È una soluzione semplice, ma, anche se la combinazione di OTP e SMS (possesso e conoscenza) sia tecnicamente conforme al requisito dei due fattori, è necessario che il dispositivo a cui viene inviato l'OTP sia sicuro. Purtroppo i numeri del cyber crime dimostrano elevati fattori di rischio .A fferma infatti Saverio Ricchiuto, Sales Director Enterprise Italia di Nuance:« I requisiti applicativi della SCA interessano il settore dei pagamenti nel suo complesso e, in particolare, tutte le istituzioni finanziarie che sono obbligate a implementare l'autenticazione forte del cliente sia negli accessi effettuati tramite internet sia in determinate operazioni».

La biometria diventa sempre più interessante in questo contesto, per l'identificazione e autenticazione del cliente, poiché è l'opzione più valida per rafforzare la sicurezza dei propri sistemi e quella dei clienti. La stessa Autorità bancaria europea raccomanda l'utilizzo dei dati biometrici per rispettare la PSD2 e aumentare la protezione di aziende e consumatori.

combinata con fattori di possesso o conoscenza, infatti, la biometria consente di raggiungere un'autenticazione a due fattori sicura.

Il ruolo della biometria

Le organizzazioni di servizi finanziari sono sempre più interessati alle tecnologie di biometria per l'identificazione e autenticazione del cliente, considerandola l'opzione più valida per rafforzare la sicurezza dei propri sistemi e quella dei clienti.

La stessa Autorità bancaria europea raccomanda l'utilizzo dei dati biometrici per rispettare la PSD2 e proteggere aziende e consumatori dalle frodi.

La biometria, infatti, combinata con fattori di possesso o conoscenza, permette di raggiungere un'autenticazione a due fattori sicura. Anche l'esperienza degli utenti, che utilizzano riconoscimento facciale e impronta digitale quotidianamente, sarà migliorata.

Le soluzioni biometriche di Nuance fra cui biometria comportamentale, vocale e riconoscimento facciale, per l'autenticazione dei clienti e il rilevamento delle frodi si basano su algoritmi di Intelligenza artificiale che abilitano, ci spiegano in azienda, un'autenticazione veloce e affidabile.

Conclude Ricchiuto:« Le aziende devono trovare il giusto equilibrio tra l'ottimizzazione dell'esperienza dei clienti e la massimizzazione della validazione di transazioni autentiche; la riduzione delle perdite legate alle frodi attraverso la rilevazione in anticipo delle transazioni fraudolente e il controllo dei costi operativi. In questo contesto, la biometria di Nuance costituisce l'alleato ideale per stabilizzare l'equilibrio e conformarsi alla PSD2, oltre a ottimizzare l'esperienza del cliente e ridurre le frodi in tutti i canali di interazione». ❖

STORMSHIELD ENDPOINT SECURITY EVOLUTION PROTEGGE LE WORKSTATION

Stormshield Endpoint Security Evolution è una soluzione per la protezione delle workstation Windows dalle minacce informatiche, anche nel cloud e in mobilità

*di **Giuseppe Saccardi***

In un mondo in cui la mobilità è diventata la norma e la tecnologia digitale permea ormai ogni settore aziendale, è sempre più importante garantire la costante protezione delle workstation, indipendentemente dal contesto in cui vengono utilizzate.

È però un obiettivo, osserva Stormshield, che comporta l'adozione di un nuovo approccio volto ad affrontare i tentativi dei cybercriminali di aggirare le soluzioni di sicurezza in essere, sfruttandone direttamente le eventuali falle.

È quello che si è proposta di ottenere con Stormshield Endpoint Security (SES) Evolution per la messa in sicurezza delle postazioni di lavoro Windows combinando la protezione adattiva comportamentale e la tecnologia di analisi dei dispositivi fornita da SES con la capacità di identificare e investigare sull'origine degli attacchi.

«La nuova generazione di attacchi avanzati – per esempio, quelli che sfruttano le vulnerabilità

zero-day – evidenzia l'incapacità della maggior parte delle soluzioni esistenti di adattarsi al contesto per fornire una protezione efficace delle workstation. La nostra soluzione Stormshield Endpoint Security Evolution fornisce una risposta pragmatica e all'avanguardia per combattere attacchi noti e non noti, contribuendo a una maggior comprensione dei team di sicurezza delle minacce che prendono di mira le loro organizzazioni», ha osservato in proposito Adrien Brochot, Product Manager di Stormshield Endpoint Security.

Considerazione di base è che quando si è in movimento, la connettività non è sempre scontata. A differenza di soluzioni che utilizzano motori di analisi ospitati su server, i cui tempi di risposta possono essere troppo lunghi in presenza di un attacco o che non sono utilizzabili se il computer è offline o al di fuori della rete aziendale, Stormshield Endpoint Security Evolution si propone di fornire una difesa permanente, che il computer sia connesso o meno. Inoltre, in alcuni ambienti sensibili, l'uso di soluzioni di sicurezza basate sul cloud può presentare rischi per la protezione dei dati. È a queste situazioni che vuole permettere di far fronte Stormshield Endpoint Security Evolution.

L'obiettivo, spiega l'azienda, è perseguito combinando le funzioni di protezione delle workstation e di rilevamento.

In pratica, Stormshield Endpoint Security Evolution blocca in modo proattivo il malware, gli attacchi alla memoria e gli exploit.

La soluzione fornisce inoltre agli amministratori informazioni che consentono di comprendere meglio come si è verificato l'attacco al fine di risalire alle sue origini

Protezione sensibile al contesto

L'approccio Zero Trust richiede che le workstation vengano tutelate in maniera diversificata a seconda del contesto d'impiego specifico (ubicazione all'interno o all'esterno della rete aziendale, utente registrato sul dispositivo, ecc.).

Stormshield Endpoint Security Evolution protegge da questo punto di vista i computer sia all'interno dell'azienda sia in un contesto di impiego mobile.

In particolare, l'agente di SES Evolution modifica dinamicamente le proprie politiche di sicurezza adattandosi al proprio ambiente, in modo da dare un accesso più granulare alle applicazioni e alle risorse dell'azienda in base all'utilizzo.

Elevata la qualità della soluzione, aggiunge Stormshield. Questo perché è stata sviluppata secondo criteri di programmazione del software difensivi e basato su un'architettura di microservizi protetta, con una protezione di livello militare contro gli attacchi che prendono di mira la soluzione di sicurezza stessa.

«Con la trasformazione delle pratiche di lavoro, garantire una protezione ottimale delle workstation è diventata una questione rilevante. La nostra soluzione è stata progettata per consentire agli amministratori di svolgere questa missione e per consentire agli utenti di lavorare in modo efficiente in un ambiente affidabile», ha osservato Brochot.❖

NAVIGARE IN SICUREZZA CON ESET INTERNET SECURITY

La soluzione sviluppata da ESET è una protezione multipiattaforma ideata per chi naviga sul web e deve proteggere dispositivi Windows, Mac, Android e Linux

*di **Giuseppe Saccardi***

Quest'anno il ritorno a scuola, così come pe ril modo di lavorare virato massicciamente verso lo smart working, si presenta molto diverso e, a prescindere che si tratti di rientro fisico o virtuale, risulta fondamentale che studenti, docenti e gli operatori siano protetti dalle minacce online.

La pandemia da Covid-19, osserva ESET, ha modificato drasticamente il sistema educativo presente e futuro, sia per i bambini in età scolare sia per gli studenti universitari. Per molti le aule virtuali hanno preso il posto di quelle fisiche, trasformando i salotti in aule e rivoluzionando i sistemi tecnologici già in atto.

Con gli studenti che si affidano a dispositivi e reti domestiche spesso condivisi da più utenti, diventa ancora più importante proteggere le reti e i dati personali e professionali.

Man mano che la scuola diventa sempre più virtuale, le preoccupazioni nel lungo periodo, per gli educatori e per gli studenti, sono quelle di preservare la privacy online e di proteggere i dati, visto che le informazioni personali, come ad esempio i voti e i rapporti comportamentali, devono essere condivise.

Per coloro che tornano in classe sarà fondamentale il rispetto delle linee guida sull'igiene e sul distanziamento sociale e gli insegnanti potranno concentrarsi sulla sicurezza fisica degli studenti più serenamente sapendo che la loro esperienza online è garantita.

ESET Internet Security offre in tal senso, ha osservato la società, una protezione da hacker, truffe e malware ed è un sistema di sicurezza a più livelli

che è volto a garantire la protezione da tutti i tipi di minacce sia online che offline.

Tra le sue caratteristiche salienti vi sono:

- Protezione multipiattaforma – Protezione di tutti i dispositivi con un'unica licenza valida per tutti i maggiori sistemi operativi (Mac, Windows, Android o Linux).
- Protezione della privacy – blocco di accessi non autorizzati ai propri dispositivi e uso improprio dei dati personali. Protezione automatica degli acquisti online e delle operazioni bancarie.
- Protezione dell'internet banking tramite uno speciale browser protetto attraverso il quale è possibile effettuare i pagamenti online in modo sicuro e accedere a portafogli crittografati basati sul web.
- Funzionalità antifurto – Consente il monitoraggio e l'individuazione del proprio pc in caso di smarrimento o furto, identificando il ladro attraverso la fotocamera integrata.
- Connessioni sicure – protezione della webcam e del router domestico dalle intrusioni. Test delle password e scansione dei dispositivi intelligenti alla ricerca di vulnerabilità.

«Sono molti gli aspetti della vita cambiati drasticamente nel corso di quest'anno, e l'istruzione non fa eccezione. La pandemia ha trasformato l'esperienza di insegnamento e apprendimento per molti in tutto il mondo, e l'ultima cosa di cui si sente il bisogno è il dover affrontare una violazione della sicurezza informatica. Siamo orgogliosi di offrire supporto a educatori e studenti con una tecnologia all'avanguardia, in grado di garantire che tutti gli utenti siano al sicuro nell'affrontare la nuova stagione scolastica», ha commentato Mária Trnková, Consumer & IoT Segment Director di ESET. ❖

ICOS POTENZIA LA DIVISIONE CYBER SECURITY

A meno di un anno dalla ricostituzione di ICOS viene annubciata la BU per la security con nuovi professionisti e un solido portfolio di soluzioni per Enterprise e PMI.

*di **Paola Saccardi***

ICOS, distributore a valore aggiunto di soluzioni infrastrutturali e sicurezza IT, ha completato la prima fase dell'implementazione della nuova divisione Cybersecurity annunciata lo scorso novembre costruendo, in 10 mesi, un solido portfolio di soluzioni per la sicurezza.

Presente sul mercato dal 1987, con sedi a Ferrara, Milano, Roma e Bolzano, ICOS ha ampliato la propria offerta di soluzioni per la Cybersecurity, già forte delle partnership con Sophos ed ESET, siglando nuovi accordi di distribuzione con Clavister, Cyberoo, DFlabs, ITsMine, i-Vertix e Safetica, con l'obiettivo dichiarato di coprire le più svariate richieste del mercato.

«ICOS, grazie agli importanti accordi di distribuzione siglati negli ultimi mesi, attraverso un'organizzazione efficiente e una riconosciuta capacità di relazione con il canale, è in grado di valorizzare vendor leader e consolidati sul mercato come Sophos ed ESET, e al tempo stesso spingere la crescita dei nuovi brand attraverso attività congiunte di enablement e affiancamento», ha commentato Federico Marini, Managing Director di ICOS.

ICOS ha rafforzato l'organizzazione dedicata alla sicurezza con l'inserimento in organico di quattro nuovi professionisti: due Product Manager, un Sales Account e un Presales Engineer. Un quinto specialista si aggiungerà a breve nell'area marketing.

Anche grazie a questo potenziamento, ha osservato ICOS, è stata in grado di avviare con soddisfazione il business relativo ai nuovi prodotti e lavorerà nei prossimi mesi per farli crescere secondo gli obiettivi, mantenendo viva l'attenzione nel valutare nuove partnership che possano ulteriormente arricchire e valorizzare il portfolio offerto.

«Proseguiremo nello scouting per identificare le eccellenze tecnologiche, sia nel nostro paese sia a livello internazionale. Stiamo sviluppando importanti sinergie anche con Sangfor, vendor globale di primo piano che è specializzato nella fornitura di soluzioni innovative di cloud computing e di network security, il cui brand pur non rientrando nella nostra divisione di Cybersecurity, si integra perfettamente nei progetti che coinvolgono la sicurezza e le soluzioni di network optimization di nuova generazione SD-WAN», ha osservato Marini. ❖

Federico Marini, Managing Director di ICOS

ANDREA NEGRONI COUNTRY LEADER CYBERSECURITY DI CISCO PER L'ITALIA

Cisco Italia ha annunciato che Andrea Negroni ha assunto la carica di Country Leader Cybersecurity di Cisco Italia. Il manager guiderà il team di esperti dedicato all'esecuzione della strategia cybersecurity di Cisco al fine di offrire a partner e clienti le migliori soluzioni e servizi

di ***Paola Saccardi***

In un momento in cui il Paese sta vivendo un grande cambiamento, la cybersecurity si conferma un tema vitale per tutte le aziende, indipendentemente dalle dimensioni e dal settore di appartenenza, spiega Cisco. Negli ultimi anni Cisco ha accelerato la propria strategia per la cybersecurity con nuove acquisizioni in questo segmento: ScanSafe nel 2009, Sourcefire nel 2013, OpenDNS nel 2015, CloudLock nel 2016, Observable Networks nel 2017, Duo Security nel 2018, fino alla più recente acquisizione di Sentryo. Una strategia confermata dalla crescita della security all'interno del fatturato aziendale, che si attesta sui 3,154 miliardi di dollari con una crescita del 10% anno su anno.

Andrea Negroni, è entrato in Cisco Italia nel 2000 e ha occupato diversi ruoli fino a ricoprire negli ultimi anni la posizione di responsabile per il go-to-market Cisco cybersecurity per i più importanti paesi dell'Unione Europea.

Andrea Negroni, Country Leader Cybersecurity di Cisco Italia

In qualità di Country Leader Cybersecurity, Andrea Negroni avrà il compito di definire le strategie di vendita, guidare il team di cybersecurity sales specialist e allineare i dipartimenti di Cisco Italia e l'ecosistema dei partner, con l'obbiettivo di incrementare il market share e di rafforzare ulteriormente la leadership di Cisco tra i vendor di Cybersecurity in Italia. ❖