

IN QUESTO NUMERO:

COVER STORY

- Una nuova sicurezza per un nuovo mondo digitale *pag. 04*
- Come allineare sicurezza, compliance e obiettivi di business *pag. 06*
- Come proteggere i dati sempre e in ogni condizione *pag. 10*
- Il SIEM evolve per essere più efficace *pag. 13*
- Fortify 20: ancora più forza alla sicurezza applicativa *pag. 16*

CYBER ATTACK

- Il questionario OAD 2020 sugli attacchi digitali *pag. 20*
- Enac, Garmin, Twitter, gli attacchi informatici non finiscono mai *pag. 22*
- Cloud e sicurezza non sempre vanno d'accordo *pag. 26*
- Più attenzione alla cybersecurity dei lavoratori da remoto *pag. 28*
- Il malware crittografato è invisibile senza l'ispezione HTTPS *pag. 30*

SOLUZIONI

- Semplificare la gestione della sicurezza aziendale *pag. 32*
- Sicurezza e affidabilità in azienda con le soluzioni Praim *pag. 35*

COVER STORY MICRO FOCUS

UNA NUOVA SICUREZZA PER
UN NUOVO MONDO DIGITALE *pag. 4*

È disponibile il nuovo libro
**IL FUTURO DEL WORKSPACE
E DELLO SMART WORKING**



Chiedi la tua copia dell'e-book scrivendo a:

shop@reportec.it • Il prezzo del libro è di 20 euro (iva inclusa)

Security & Business 54
luglio-agosto 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

di Gaetano Di Blasio

I RISCHI DI UN MONDO SEMPRE PIU' DIGITALE

Il numero 54 di Security&Business presenta una nuova cover story di Micro Focus, nota azienda di software con una grande tradizione legata alle soluzioni per la cyber security, un elemento fondamentale per la crescita del mondo digitale, minacciato dagli attacchi ai sistemi informatici e alla privacy di individui e organizzazioni.

A seguire la cover story, troviamo la caratteristica rubrica sugli attacchi informatici e le tendenze di questo mondo. In particolare Cyber Attack fornisce un breve, ma esauriente resoconto di alcuni fra più recenti attacchi informatici che hanno avuto un impatto molto importante, soprattutto per l'importanza delle aziende coinvolte, a cominciare da Twitter. Una compromissione che coinvolge uno strumento adoperato, nel bene e nel male da "influencer" in grado di spostare le scelte di masse significative, per esempio decretando il successo di un prodotto commerciale. Peraltro un "cinguetto" di Donald Trump potrebbe innescare una guerra.

Anche senza arrivare a questi eccessi i rischi alla sicurezza possono produrre danni, fossero soli quelli alla propria reputazione e altri che bloccano operazioni quotidiane, come nel caso di Garmin o, in Italia, quelle dell'Enac, che gestisce i voli dell'aviazione civile.

I cyber criminali, anche grazie all'ausilio di strumenti basati sul machine learning, sono sempre pronti ad approfittarne. Senza contare gli attacchi mirati, spesso attivati attraverso una semplice email. Di queste ultime occorre diffidare, soprattutto quando eventi, quali la pandemia o anche un evento sportivo, attraggono l'attenzione mediatica.

Il digitale sarà sempre più protagonista della vita quotidiana, come evidenzia nella cover story, Pierpaolo Ali, sottolineando che le condizioni sociali imposte dalla pandemia Covid19 hanno decisamente accelerato un processo di trasformazione già in atto, portando gli strumenti digitali in ogni aspetto della vita comune. In questo contesto, la sicurezza digitale assume, ormai, una valenza universale, che si estende oltre il tema dei rischi economici per diventare elemento abilitante del nuovo mondo digitale.

Il numero 54 presenta, infine alcune delle soluzioni proposte sul mercato business to business.

UNA NUOVA SICUREZZA PER UN NUOVO MONDO DIGITALE

Pierpaolo Ali, Director Southern Europe Security, Risk & Governance di Micro Focus analizza l'evoluzione della sicurezza digitale e spiega perché identità, dati, applicazioni sono il fulcro per una protezione efficace basata sul machine learning

di Riccardo Florio



Come cambia lo scenario della sicurezza digitale?

Pierpaolo Ali' (P.A.): Le condizioni sociali imposte dalla pandemia Covid19 hanno notevolmente accelerato un processo di trasformazione già in atto, portando gli strumenti digitali in ogni aspetto della vita comune, dalle videochiamate, alle visite ai musei virtuali, dalle prescrizioni di farmaci, ai corsi online. La sicurezza digitale assume, ormai, una valenza universale, che si estende oltre il tema dei rischi economici per diventare elemento abilitante del nuovo mondo digitale.

Per le aziende questo cosa significa?

P.A.: Le aziende che operano in un mondo digitale devono intraprendere, a loro volta, un processo di trasformazione digitale. Molte hanno già avviato questo percorso, orientandosi verso modelli di servitization in cui la componente digitale entra nel core business. Altre ancora hanno radicalmente reinventato il loro business in modo digitale: basti pensare che la più importante azienda di hospitality, Airbnb,

non possiede strutture alberghiere così come una delle più grandi aziende di trasporto, Uber, non dispone di un parco autoveicoli.

Per le aziende, la sicurezza informatica diventa, di conseguenza, protezione irrinunciabile del proprio business.

Quali sono le nuove sfide da affrontare?

P.A.: Il numero di rischi da affrontare è in costante aumento. Tuttavia, non si tratta solo dell'impressionante incremento numerico delle minacce da fronteggiare, quanto piuttosto della loro natura. Gli attacchi sono sempre più sofisticati e spesso vengono perpetrati sfruttando credenziali legittime sottratte con strumenti di social engineering. Gli attaccanti riescono ad accedere a informazioni sensibili e a copiare documenti in modo indisturbato a volte anche per molti mesi prima di essere individuati. Per questo motivo anche gli strumenti di protezione devono mutare.

In passato l'atteggiamento verso la sicurezza era

reattivo e le soluzioni di protezione intervenivano quando il danno era già stato fatto. Si è poi passati a un atteggiamento preventivo con l'utilizzo di tecnologie più sofisticate come gli IPS (Intrusion Prevention System) di nuova generazione. Ma oggi serve qualcosa in più: una sicurezza predittiva e intelligente, guidata da nuove tecnologie di machine learning capaci di identificare in tempo reale ogni situazione anomala e di rispondere immediatamente bloccando l'accesso e isolando risorse.

Quali sono i passi per introdurre in azienda una protezione efficace?

P.A.: Il primo punto su cui è necessario avere consapevolezza è che il perimetro aziendale, così come veniva pensato e protetto in passato, non esiste più. L'accesso a dati e risorse aziendali avviene sempre e da ogni luogo e ciò che definisce il nuovo perimetro di sicurezza sono le identità digitali degli utenti e i privilegi associati. Una protezione efficace passa attraverso un'adeguata governance delle identità e un approccio di Zero Trust Security, che non prevede l'assegnazione di alcun privilegio aggiuntivo oltre a ciò che è strettamente necessario per svolgere il proprio lavoro.

In secondo luogo, la protezione dei dati, in cui risiede il patrimonio di conoscenza e di relazioni di un'azienda, va rafforzata, estendendola al loro intero ciclo di vita. Questo significa garantirne la cifratura in ogni situazione: quando sono archiviati, mentre vengono trasferiti, ma anche durante l'utilizzo. Quest'ultima è un'esigenza cruciale a cui solo Micro Focus, grazie alle tecnologie esclusive e brevettate inserite nelle soluzioni Voltage, è in grado di fornire un'efficace risposta.

Infine, si deve porre attenzione alle applicazioni che

sono il cuore del business ma che, troppo spesso, non sono adeguatamente testate durante il processo di sviluppo o una volta entrate in produzione, per proteggersi da ogni possibile vulnerabilità.

Qual è la proposta di Micro Focus per una nuova sicurezza?

P.A.: Micro Focus propone una protezione completa, integrata, modulare attraverso una gamma di soluzioni software organizzate in famiglie specifiche. Tutte le soluzioni Micro Focus sono integrabili tra loro e con soluzioni di terze parti, per abilitare un approccio di sicurezza efficace e favorire, nel contempo, un percorso di aggiornamento che garantisca la protezione degli investimenti già effettuati. Alla protezione delle applicazioni si indirizza la gamma di soluzioni Fortify pensata per favorire uno sviluppo sicuro e predisporre test statici e dinamici sia sui software sviluppati internamente sia su quelli acquisiti da terze parti.

ArcSight è la famiglia di soluzioni pluripremiata che fornisce protezione in tempo reale contro gli attacchi noti e sconosciuti, sfruttando la tecnologia di machine learning non supervisionato Micro Focus Interset.

Le soluzioni NetIQ mettono a disposizione tutti i tasselli per predisporre una governance sicura dell'accesso e dell'identità che favorisce i modelli di smart working, mentre le soluzioni Voltage Data Security forniscono la cifratura dei dati dal momento della loro creazione fino alla loro cancellazione sicura.

L'insieme delle soluzioni di Security, Risk & Governance di Micro Focus fornisce gli elementi per implementare una protezione efficace, predittiva, prescrittiva e intelligente necessaria per il nuovo mondo digitale.



COME ALLINEARE SICUREZZA, COMPLIANCE E OBIETTIVI DI BUSINESS

Coniugare, compliance, gestione dell'identità e obiettivi aziendali è un obiettivo arduo che richiede un approccio integrato e automatizzato alla compliance basato su solidi principi di sicurezza. Micro Focus risponde a questa sfida con la famiglia di soluzioni NetIQ

di Riccardo Florio

Secondo lo studio di Ponemon 2019, Cost of a Data Breach (relativo a dati raccolti in 16 Paesi tra luglio 2018 e aprile 2019) il costo medio globale di una violazione dei dati è di circa 3,92 milioni di dollari, in aumento dell'1,5% rispetto al 2018. In Italia questo costo si attesta a 3,52 milioni di dollari, mentre negli Stati Uniti sale fino a 8,19 milioni di dollari. Peraltro, dallo studio emerge che l'impatto sull'azienda di una violazione prosegue per anni: circa un terzo dei costi valutati da Ponemon si è verificato più di un anno dopo la violazione.

Dei 26 fattori considerati da Ponemon nella valutazione del costo, i tre che hanno contribuito maggiormente sono risultati: il coinvolgimento di terzi (+370mila dollari rispetto al valore medio), errori di compliance (+350mila dollari), migrazione estesa al cloud (+300mila dollari).

Questi dati sono la naturale conseguenza di uno scenario in cui l'azienda si apre sempre più verso l'esterno con dati che si spostano oltre i confini della rete interna.



La nuova sfida per le aziende è implementare un programma di compliance sostenibile, in grado di adattarsi rapidamente al mutamento dei requisiti normativi, della tecnologica e dei modelli di business, migliorando, nel contempo, la condizione di sicurezza aziendale generale e la gestione delle identità digitali.

Controlli armonizzati e automazione per una compliance sostenibile e adattativa

La base di un programma sostenibile di sicurezza e compliance richiede, innanzitutto, la predisposizione di un framework comune e armonizzato di obiettivi di controllo creati sulla base di best practice; mano a mano che l'ambiente normativo evolve, è possibile aggiungere controlli a questo insieme comune, consentendo all'azienda di adattare rapidamente il



proprio programma di conformità.

I controlli di compliance devono essere definiti all'interno di un programma esteso di mitigazione del rischio capace di adattarsi non solo ai mutevoli requisiti di compliance, ma anche all'evoluzione delle minacce.

Gli attacchi, infatti, evolvono costantemente nel metodo e negli obiettivi. Le motivazioni primarie degli attacchi sono ora finanziarie e politiche e gli aggressori sono anche diventati più professionali e organizzati: reclutano talenti, investono in ricerca e sviluppo e producono strumenti nuovi e sempre più avanzati.

Ecco perché l'introduzione di elementi di automazione nella attività di monitoraggio, raccolta dei dati, analisi e controllo diventa indispensabile per garantire il rispetto delle policy, ridurre l'errore umano e diminuire i costi.

I nuovi modelli di lavoro cambiano lo scenario di rischio

Oltre alla naturale evoluzione degli attacchi, i team di sicurezza devono anche far fronte alle sfide di un perimetro sempre più dinamico e indefinito.

La forza lavoro è sempre più diversificata e dinamica e un numero maggiore di persone ha, oggi, accesso direttamente o indirettamente a informazioni sensibili o ai sistemi e alle applicazioni che le ospitano. La tipologia di utenti considerabili "interni" include il personale dei partner, i fornitori di servizi gestiti e di hosting i cloud service provider e molte aziende non attuano le verifiche idonee per appurare che tutti questi soggetti aderiscano ai propri obiettivi di controllo.

In questo ambiente dinamico, il rischio che l'attività di un utente interno contribuisca alla violazione dei dati è decisamente in aumento. Qualunque sia il tipo di utente i rischi associati ad attività intenzionali, inappropriate o involontarie possono essere significativamente ridotti attraverso controlli relativamente semplici. Un semplice esempio di controllo è una policy per garantire che l'account di un dipendente sia disabilitato contestualmente alla sua uscita dall'azienda.

In questo scenario incentrato sui dati, con minacce in evoluzione e perimetri indefiniti, si afferma, dunque, l'efficacia di un modello di **Zero Trust Security** che, implicitamente, riconosce che gli addetti ai lavori non sono più solo i dipendenti e che il nuovo

perimetro aziendale da proteggere si chiama identità. Tutte le attività devono essere monitorate, il livello di accesso fornito deve essere sempre quello minimo necessario e si deve monitorare costantemente come vengono sfruttati i privilegi.

Micro Focus tramite la famiglia di prodotti NetIQ mette a disposizione gli strumenti per realizzare una gestione Zero Trust dell'identità e dell'accesso adatta per le aziende che vogliono di raggiungere i propri obiettivi di compliance mantenendo un ambiente sicuro e allineato agli obiettivi aziendali.

Identity governance e amministrazione

Alle esigenze di Identity governance e amministrazione si indirizzano **NetIQ Identity Governance** e **NetIQ Identity Manager**.

La prima è una soluzione di controllo e certificazione dell'accesso adatta a rispondere alle esigenze di compliance e ridurre proattivamente i rischi. NetIQ Identity Governance mette a fattor comune tutte le informazioni sui diritti degli utenti legate a sistemi, applicazioni e dati, per verificare se i privilegi di accesso esistenti sono appropriati. La sua peculiarità è la capacità di esercitare una governance capace di adattarsi in tempo reale ai cambiamenti e agli eventi.

Micro Focus NetIQ Identity Manager è il framework per una gestione centralizzata delle identità digitali, che effettua in modo automatizzato un continuo processo di confronto e allineamento tra i dati di accesso presenti nei sistemi IT e i permessi, con la capacità di eseguire automaticamente azioni quali

il provisioning dei privilegi minimi, il de-provisioning e le opzioni self-service per le richieste e le approvazioni degli accessi.

Gestione dell'accesso dei privilegi

Alla gestione dell'accesso sicuro Zero Trust si indirizza NetIQ Access Manager, una soluzione che fornisce funzionalità di Single Sign-On su Web mettendo a disposizione un unico accesso sicuro a intranet e applicazioni basate su cloud da qualsiasi luogo, per qualsiasi utente e tramite qualunque dispositivo. Garantisce le interazioni sicure con i partner sui dispositivi mobili, abilitando le App native o estendendo su di essi le applicazioni basate sul Web.

In un ambiente ibrido complesso può, inoltre, essere molto difficile identificare tutte le identità che dispongono di diritti di accesso privilegiati. Per semplificare questo compito Micro Focus ha sviluppato una serie di soluzioni.

NetIQ Privileged Account Manager individua le credenziali con privilegi elevati in azienda, traccia e registra le corrispondenti attività e dipendenze, mettendo a disposizione le informazioni necessarie per rivedere le policy di accesso.

NetIQ Directory and Resource Administrator media l'accesso a Microsoft Active Directory, limitando l'utente a particolari azioni per visualizzazioni specifiche dell'intera directory. Questa soluzione esegue processi automatizzati tra cui il provisioning degli utenti, favorisce il consolidamento delle directory, il rispetto delle policy di sicurezza e la

Zero Trust Security

Il modello Zero Trust Security prevede di non fidarsi mai e verificare sempre. Adottare questo approccio significa ribaltare il presupposto che tutto ciò che si colloca dietro il firewall aziendale sia sicuro, considerando ogni richiesta di accesso come se provenisse da una rete aperta e potenzialmente rappresentasse un tentativo di violazione.

Pertanto, ogni richiesta deve essere autenticata e autorizzata, indipendentemente dalla sua provenienza o dalla risorsa a cui si intende accedere.

In aggiunta, il modello Zero Trust sposa i principi della micro-segmentazione per ridurre i possibili rischi correlati ai movimenti laterali e dell'assegnazione di privilegi minimi in modo che non esista una condizione in cui la fiducia affidata a dipendenti e partner per connettersi tra loro e collaborare possa superare i limiti imposti dai propri compiti lavorativi.

segregazione dei compiti.

NetIQ Change Guardian monitora in tempo reale file, sistemi e applicazioni critiche per rilevare attività privilegiate non autorizzate e notificare in tempo reale ogni modifica non autorizzata ai file, alle piattaforme e ai sistemi essenziali, fornendo informazioni dettagliate su file, directory, condivisioni di file, chiavi di registro (su Windows), processi di sistema e altro ancora. Soddisfa i requisiti di governance e di conformità dimostrando la capacità di monitorare l'accesso ai file e ai dati critici. ❖



COME PROTEGGERE I DATI SEMPRE E IN OGNI CONDIZIONE

Dati protetti in ambienti ibridi, archiviati, in movimento, in uso, attraverso l'intero ciclo di vita e anche quando si trovano nei file destrutturati: questo è ciò che promettono le soluzioni Micro Focus Voltage SecureData

di Vittorio Destino

I dati vanno protetti sempre e comunque: si tratta di un imperativo condiviso ormai da analisti, produttori e utenti finali.

Il compito, però, non è facile perché i dati critici vanno protetti in ogni condizione (a riposo, in movimento e durante l'uso), attraverso il loro intero ciclo di vita, in ambienti ibridi che si estendono attraverso il cloud e la rete mobile, perché sono sempre più spesso Big Data e perché un numero sempre più ampio di dati aziendali critici sono contenuti all'interno di file di natura destrutturata.

Protezione in ambienti ibridi in ogni condizione

La famiglia Voltage SecureData di Micro Focus mette a disposizione strumenti per la cifratura dei dati attraverso un'infrastruttura comune e condivisa che prevede gli stessi server centralizzati e i medesimi strumenti di amministrazione. Questo obiettivo viene conseguito attraverso un modello dato-centricò che prevede di implementare il meccanismo di difesa e protezione direttamente sul dato o sui sistemi che lo trattano. In tal modo, i dati restano sempre

cifrati dal momento della loro creazione fino alla loro cancellazione sicura.

Al centro delle soluzioni Voltage SecureData vi sono una serie di tecnologie innovative e brevettate di cifratura e di accesso sicuro che garantiscono una protezione che segue i dati sempre, in ogni condizione e attraverso ogni ambiente.

Tecnologie uniche e innovative

Grazie alla tecnologia Stateless Key Management, le soluzioni Micro Focus Voltage risolvono una serie di problemi legati all'affidabilità e alla gestione delle chiavi di cifratura. Il processo di generazione e rigenerazione della chiave di cifratura avviene, infatti, in modalità on-demand senza dover mantenere l'archivio delle chiavi che, tipicamente, è destinato a crescere rendendo più difficile l'amministrazione e aumentando i costi IT.

Un'altra caratteristica distintiva delle soluzioni Micro Focus Voltage è Hyper SST (Secure Stateless Tokenization), una tecnologia di tokenizzazione pensata per le esigenze di sicurezza dei dati delle carte di pagamento. La sua particolarità è di non

richiedere la presenza di un database per la memorizzazione dei token e di non prevedere neppure la memorizzazione dei dati del titolare della carta o altri dati sensibili. Queste caratteristiche contribuiscono ad aumentare la velocità di conversione, la scalabilità, la sicurezza e la gestibilità del processo di tokenizzazione con conseguenti risparmi nei costi.

Dati cifrati anche durante l'utilizzo

Utilizzare i dati in chiaro quando sono utilizzati dalle applicazioni sembrerebbe una richiesta ineludibile. Micro Focus ha superato questa limitazione sviluppando Hyper Format-Preserving Encryption (Hyper

FPE) uno standard di cifratura riconosciuto dal NIST e brevettato che permette di cifrare i dati preservandone il formato originale ovvero la loro integrità referenziale. Questo permette alle applicazioni, ai processi di analytics e ai database di utilizzare i dati protetti senza alterazioni.

I dati strutturati come codice fiscale, carta di credito, numero di conto corrente, data di nascita, indirizzi di posta elettronica possono essere crittografati direttamente nel momento in cui vengono prodotti. Una volta cifrati, questi dati possono ancora essere referenziati e uniti in modo consistente attraverso tabelle e data set: si tratta di un requisito molto

Cifratura, tokenization, data masking

La cifratura prevede la codifica dei dati originali (cosiddetti in chiaro) attraverso sofisticati algoritmi che li convertono in un formato illeggibile. Tramite un'opportuna chiave di decifratura è possibile ripristinare il formato originale dei dati.

Anche la tokenizzazione rende illeggibile il dato originale ma, a differenza della cifratura, il valore originale viene sostituito da un valore alfanumerico generato casualmente, chiamato token. Un opportuno server memorizza le relazioni tra i valori originali e il token e, quando un'applicazione deve accedere ai dati originali, il sistema di tokenizzazione cerca il valore del token per recuperarlo e ricreare l'associazione inversa.

Il data masking è un altro metodo per rendere illeggibili i dati modificandone il contenuto. Può assumere una forma semplice in cui i dati reali sono sostituiti con valori nulli o costanti oppure forme più sofisticate in cui i dati vengono alterati mantenendone però il formato originale, così da preservare la possibilità di eseguire su di essi operazioni di analisi senza il timore di perdere informazioni riservate.

importante quando vengono, per esempio, utilizzati identificatori comuni come il codice fiscale o la carta di identità come riferimenti comuni tra insiemi di dati diversi.

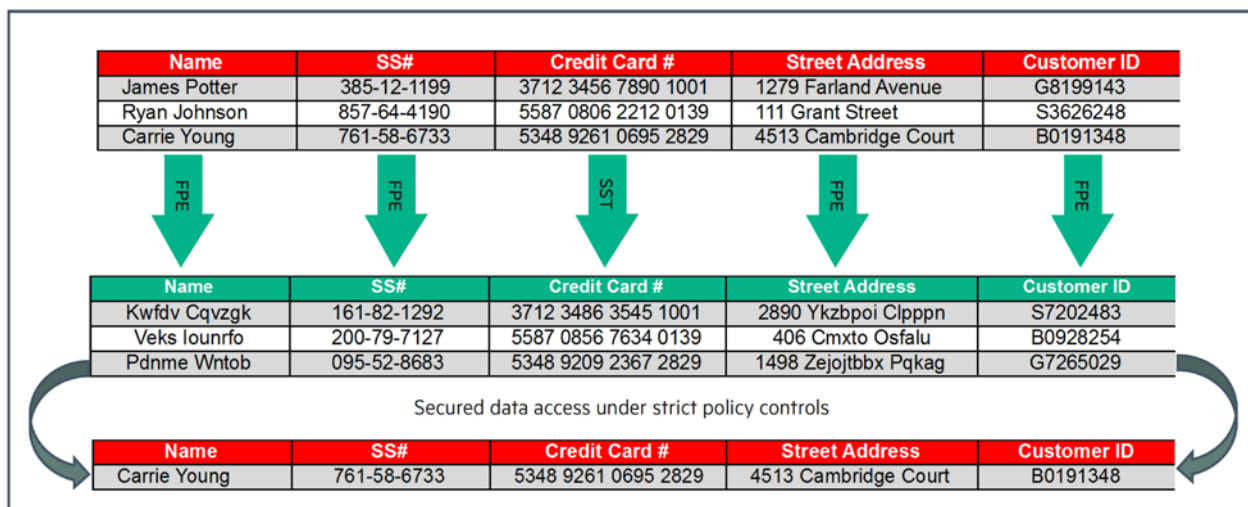
Protezione per file e dati non strutturati

Il più recente tassello della famiglia di soluzioni Micro Focus Voltage si chiama SmartCipher ed è stato sviluppato per proteggere i file non strutturati e i dati critici contenuti al loro interno.

«Il portafoglio di soluzioni Micro Focus Voltage protegge i dati sensibili e abilita controlli granulari, riducendo il rischio di violazione della privacy - osserva **Pierpaolo Ali, Director Southern Europe Security, Risk & Governance di Micro Focus** -. L'introduzione sul mercato di Voltage SmartCipher mette a disposizione dei nostri clienti la possibilità di gestire e proteggere in modo completo anche le informazioni sensibili contenute nei file non

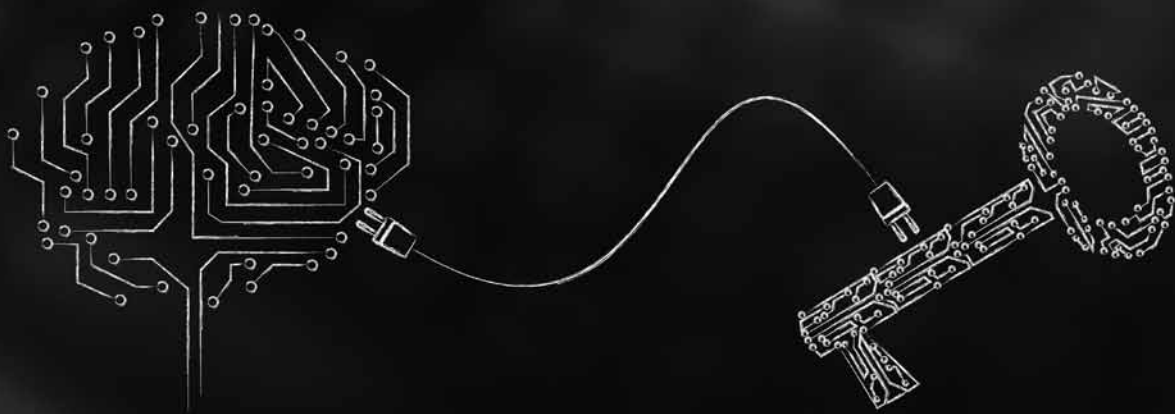
strutturati, mantenendo il costante controllo sul loro accesso e utilizzo. Tutto questo in modo trasparente per l'utente e senza creare discontinuità nell'ambiente di security preesistente».

Voltage SmartCipher permette di applicare ai file una protezione persistente tramite un algoritmo di cifratura AES-256, che li segue attraverso qualsiasi tipo di piattaforma durante il loro intero ciclo di vita. Ai file e ai dati contenuti al loro interno sono aggiunte policy di accesso e protezione. In tal modo, attraverso un sistema centralizzato di "policy management", è possibile costantemente individuare i file, monitorare il loro utilizzo, modificare i criteri di controllo e prevenire l'accesso non autorizzato per mantenerli sempre protetti, ovunque si trovino. Voltage SmartCipher è disponibile sia come prodotto in licenza per l'endpoint oppure in forma di abbonamento annuale. ❖



Esempio di come operano le tecnologie Hyper FPE (Format-Preserving Encryption) e Hyper SST (Secure Stateless Tokenization)

IL SIEM EVOLVE PER ESSERE PIÙ EFFICACE



Integrazione della tecnologia Intersect di machine learning non supervisionato, aggiunta di una piattaforma SOAR e separazione in due componenti per ArcSight ADP sono tra le ultime novità della piattaforma SIEM di Micro Focus

di Vittorio Destino

ArcSight è la soluzione SIEM di Micro Focus adatta alle esigenze delle aziende enterprise che devono analizzare in tempo reale grossi flussi di dati. ArcSight prevede molteplici use case di compliance pronti all'uso e incorpora il framework MITRE ATT&CK per un'analisi completa degli eventi di sicurezza.

Alla componente "core" del SIEM denominata Arcsight Enterprise Security Manager (ESM) si affiancano strumenti di raccolta e gestione dei dati, tecnologie per l'analisi delle anomalie di comportamento e soluzioni per l'investigazione e la gestione degli incidenti.

Per incrementare il livello di flessibilità, la precedente componente di raccolta e gestione denominata ArcSight Data Platform (ADP) è stata recentemente suddivisa in due componenti autonome separate: Logger e Security Open Data Platform (SODP).

Logger è una soluzione per la gestione e la ricerca dei log di registro. La Security Open Data Platform mette a disposizione Smart Connector per connettersi a più di 450 tipi di fonti dati e per raccogliere, aggregare, pulire e arricchire i dati prima di inserirli nelle analisi di sicurezza. SODP include Transformation Hub, che è capace di estrarre centinaia di migliaia di eventi al secondo.

Con la recente acquisizione di ATAR Labs Micro Focus ha anche integrato nella sua offerta SIEM funzionalità native SOAR g (vedi box).

Interset: Machine learning per l'analisi dei comportamenti

Interset è il più recente tassello tecnologico integrato nell'offerta Security, Risk & Governance di Micro Focus, a seguito dell'acquisizione dell'omonima azienda canadese.

Si tratta di un software per l'analisi di sicurezza di tipo predittivo che utilizza tecnologie di Machine learning non supervisionato per integrare all'interno di ArcSight funzioni di analisi comportamentale

degli utenti e delle entità (User and Entity Behavioural Analytics, in sigla UEBA).

La tecnologia Interset dispone di un motore di analytics che integra oltre 200 algoritmi ed è stata sviluppata sulla base dell'analisi di "use case" reali. Si avvale di una libreria di oltre 350 modelli e analizza enormi quantità di dati, imparando in modo sempre più raffinato a riconoscere le normali modalità di comportamento di ogni utente, ogni macchina, ogni stampante, ogni indirizzo IP, ogni entità all'interno dell'ambiente IT. Interset genera un punteggio di rischio confrontando i comportamenti attuali con quelli passati e quelli di figure professionali analoghe per identificare comportamenti insoliti che potrebbero

Una nuova soluzione SOAR per Micro Focus

Micro Focus ha acquisito ATAR Labs, azienda che ha sviluppato la soluzione Atar di Security Orchestration, Automation and Response (SOAR). Questa soluzione è stata integrata con ArcSight negli ultimi anni e diventa ora un asset interno di Micro Focus favorendone lo sviluppo futuro e l'integrabilità con le sue soluzioni di governance e security. ATAR è una tecnologia che aiuta le aziende a radunare centralmente gli avvisi e i feed di minacce e ad attivare automaticamente azioni di risposta e ripristino. Le sue funzionalità consentono, tra l'altro, di interrogare endpoint, configurare firewall, isolare computer in una rete, bloccare account utente (temporaneamente o permanentemente). L'uso di questa soluzione SOAR può ridurre i tempi di indagine da ore a minuti e di avviare azioni automatiche di risposta in tempi estremamente rapidi.



presentare un potenziale rischio per la sicurezza. Interset prevede un'architettura scalabile capace di combinare il proprio motore di analisi avanzata con tecnologie open source per la gestione dei Big Data, incluse Kafka, Spark, Phoenix, Hadoop, HBase, Elasticsearch, ZooKeeper, d3 e Kibana.

ArcSight Investigate e Fusion 1.0

ArcSight Investigate è la componente indirizzata agli analisti di sicurezza, sviluppata per aumentare la rapidità di intervento e la capacità di analisi, finalizzata alla ricerca e all'investigazione di possibili minacce alla sicurezza. Permette di elaborare in tempo quasi istantaneo enormi quantità di dati

fornendo capacità di analisi dei big data di sicurezza e di definire le priorità di intervento.

La versione 2020 di ArcSight segna anche l'esordio di Fusion 1.0, la nuova interfaccia utente intuitiva che mette a disposizione una dashboard con una serie di widget personalizzabili. Fusion consente di visualizzare, identificare e analizzare potenziali minacce incorporando informazioni di intelligence provenienti da:

- attività di monitoraggio e correlazione degli eventi in tempo reale con i dati di ArcSight ESM;
- analisi del comportamento dell'utente finale con ArcSight Interset;
- esecuzione di indagini approfondite effettuate con ArcSight Investigate. ❖



MITRE ATT&CK

MITRE ATT&CK è una base di conoscenza globale aperta, gratuita e disponibile a tutti di tattiche e tecniche di difesa basate su esperienze e osservazioni del mondo reale. Può essere utilizzata come base per lo sviluppo di specifiche metodologie e per la definizione di modelli di minacce da parte di aziende private, Pubblica Amministrazione e per la definizione di prodotti e servizi di sicurezza informatica. Il framework MITRE ATT&CK è disponibile da anni ma sta assumendo una crescente diffusione e adozione da parte delle aziende sotto l'esigenza di rafforzare la sicurezza IT. MITRE ATT&CK è la mappa ideale per identificare quali dati, log ed eventi devono essere analizzati dal SIEM, per scoprire le minacce, monitorare la sicurezza e investigare gli incidenti.

FORTIFY 20: ANCORA PIÙ FORZA ALLA SICUREZZA APPLICATIVA

La versione 20 di Fortify rafforza la posizione di primato della suite di prodotti Micro Focus per la sicurezza delle applicazioni confermata da Gartner nei suoi recenti rapporti. Tra le novità la stretta integrazione con Sonatype per la sicurezza dei codici open source

di Vittorio Destino

La versione 20 di Fortify amplia le funzionalità della suite di Micro Focus per la sicurezza delle applicazioni che si conferma per il settimo anno consecutivo tra i leader nel Gartner Magic Quadrant for Application Security Testing oltre a figurare al primo posto nel rapporto 2020 Gartner Critical Capabilities for Application Security Testing per i casi d'uso Enterprise e Mobile and Client. Gartner premia Fortify conferma l'accuratezza e profondità dei suoi risultati, la flessibilità e l'efficacia nelle attività



PENETRATION TEST

COMPONENT	VERSION	TYPE	KNOWN PUBLIC VULNERABILITIES				LICENSE	RELEASES
			CRITICAL	HIGH	MEDIUM	LOW		
org.apache.geronimo.framework.geronimo	2.1	maven	1	0	3	0	Apache-2.0	2
ch.qos.logback.logback-access	0.6	maven	1	0	0	0	LGPL-3.0	2
tomcat/hamcat-util	5.5.23	maven	0	1	4	0	Apache-2.0	2
org.mortbay.jetty/jetty	6.1.15	maven	0	1	4	0	Apache-2.0	2
apache-httpclientcommons-httpclient	3.1	maven	0	1	2	0	Apache-2.0	2
commons-beanutils/commons-beanutils	1.8.3	maven	0	1	0	0	Apache-2.0	2
geronimo/geronimo-tomcat	1.0	maven	0	1	0	0	Apache-2.0, Not Declared	2

Vista di un'analisi SCA all'interno di Fortify on Demand

di sostituzione di codici legacy, nelle modalità moderne di sviluppo (per esempio microservizi) unitamente a funzionalità di reporting e integrazione di classe enterprise.

Le ultime novità introdotte ampliano le funzionalità indirizzate agli sviluppatori per la sicurezza dei Container e prevedono un ampliamento dei linguaggi di programmazione supportati tra cui Kotlin e COBOL. Micro Focus ha anche rafforzato la sua partnership con Sonatype attraverso un accordo OEM e l'integrazione all'interno del servizio di test in cloud Fortify on Demand (FoD) della sua piattaforma di Software Composition Analysis (SCA). La soluzione SCA di Sonatype, basata sul motore di machine learning Nexus Intelligence, consente di effettuare un'analisi automatica durante l'uso dei software open source ai fini della gestione del rischio, della sicurezza e della compliance.

Le azioni di sviluppo delle soluzioni Micro Focus

Fortify continuano a indirizzarsi verso il rafforzamento di un modello di sviluppo che pone al centro lo sviluppatore e orientato alla metodologia DevSecOps.

DevSecOps

L'esperienza sul campo ha evidenziato che, per sfruttare efficacemente i vantaggi offerti dalla metodologia di sviluppo DevOps, è necessario tenere conto degli aspetti di sicurezza attraverso l'intero ciclo di vita delle applicazioni. Il termine DevSecOps sottolinea l'integrazione degli aspetti di sicurezza delle applicazioni e dell'infrastruttura fin dall'inizio del ciclo di sviluppo e l'automazione alcune attività di controllo al fine di creare una base sicura per le iniziative di sviluppo DevOps.

SAST, DAST, IAST e MAST

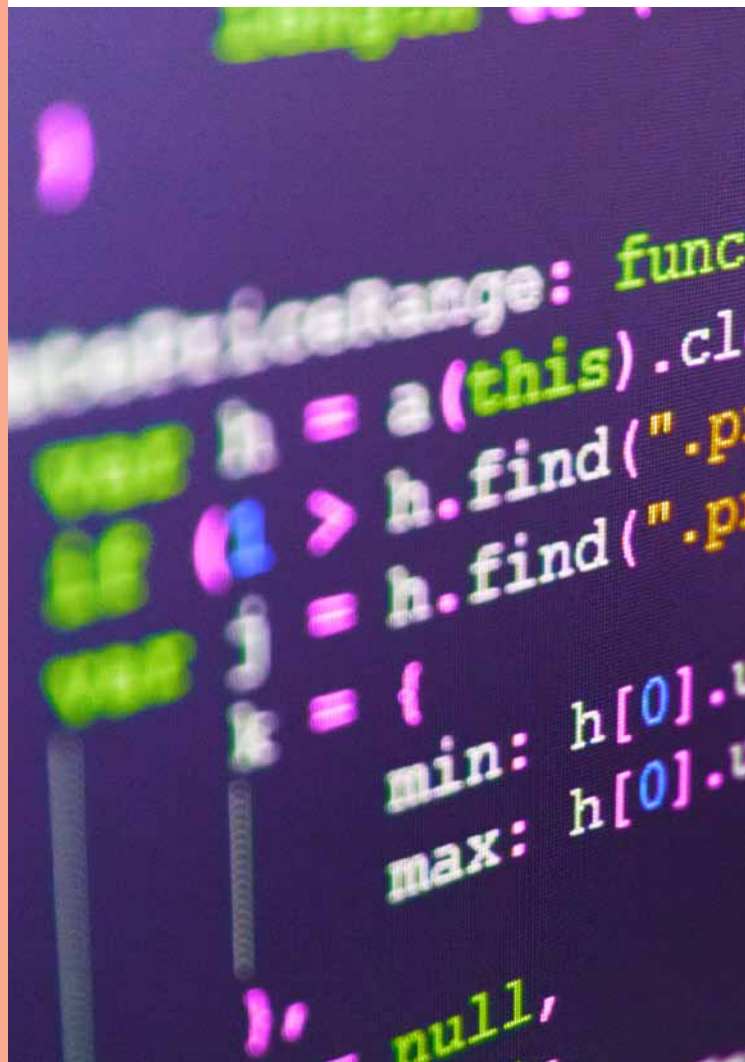
SAST è la sigla di Static Application Security Testing e indica le soluzioni per effettuare test di sicurezza delle applicazioni in modalità statica eseguendo una scansione del codice sorgente per individuare possibili vulnerabilità.

DAST, acronimo di Dynamic Application Security Testing, fa riferimento a test effettuati su applicazioni o servizi Web in esecuzione, attraverso sistemi di scansione automatica e attacchi controllati simulati, per identificare le vulnerabilità sfruttabili in un ambiente in esecuzione e i punti deboli dell'architettura

IAST sta per Interactive Application Security Testing ed è una tecnica che combina SAST e DAST. Effettua l'analisi del codice sorgente alla ricerca di vulnerabilità della sicurezza mentre l'applicazione viene messa in esecuzione da un test automatizzato, da un operatore addetto ai test o da qualsiasi attività che interagisca con le funzionalità dell'applicazione.

Mobile AST (MAST) indica le attività di test delle applicazioni in ambiente mobile simulando i principali attacchi ed effettuando un assessment capace di estendersi all'intero stack tecnologico: client, rete e server.

L'obiettivo è di arrivare ad abilitare un flusso di lavoro integrato completamente automatizzato. In questa direzione si inseriscono: un maggiore spostamento delle attività DAST nelle mani dello sviluppatore portando all'interno dell'ambiente di sviluppo l'interazione tra le scansioni FoD e il codice sorgente; l'aggiunta di nuove funzionalità di automazione tra cui l'auto generazione delle macro; la disponibilità di API RESTful documentate con Swagger.



Le soluzioni Fortify per la sicurezza applicativa

Il modello di protezione proposto da Fortify è di tipo adattativo, con un programma di sicurezza applicativa di tipo centralizzato in grado di intervenire in ambienti ibridi che includono soluzioni on-premise, mobili e in cloud.

La famiglia di soluzioni Fortify comprende Static Code Analyzer (SAST) e WebInspect (DAST e IAST)



per il test statico e dinamico delle applicazioni. Il servizio Fortify on Demand abilita anche funzionalità di MAST rispetto a tutti i vettori di attacco mobile con la possibilità di integrare i risultati della scansione con gli strumenti di reporting Fortify.

Fortify Audit Workbench (AWB) è un'applicazione complementare a Micro Focus Fortify Static Code Analyzer che mette a disposizione un'interfaccia grafica per analizzare e organizzare i risultati della scansione, aggiungere dati di audit, applicare filtri ed eseguire semplici report.

La famiglia comprende anche Application Defender, che consente di sviluppare applicazioni basate su tecnologia RASP (Runtime Application Self-Protection) ovvero dotate di meccanismi di auto-protezione da attacchi e vulnerabilità.

Tutte le soluzioni possono essere gestite attraverso Fortify Software Security Center, un repository di gestione centralizzato che fornisce visibilità sull'intero programma di sicurezza delle applicazioni dell'azienda per aiutare a eliminare le vulnerabilità di sicurezza che interessano il software.

La gamma Fortify include anche funzionalità per:

- realizzare scansioni statiche su larga scala (ScanCentral);
- garantire uno sviluppo sicuro (Security Assistant);
- effettuare operazioni automatizzate di auditing sfruttando il machine learning (Audit Assistant) con la flessibilità di rivedere manualmente le previsioni di intelligenza artificiale sui problemi o di optare per previsioni automatiche;
- ridurre i falsi positivi (Cleans Rules).



IL QUESTIONARIO OAD 2020 SUGLI ATTACCHI DIGITALI

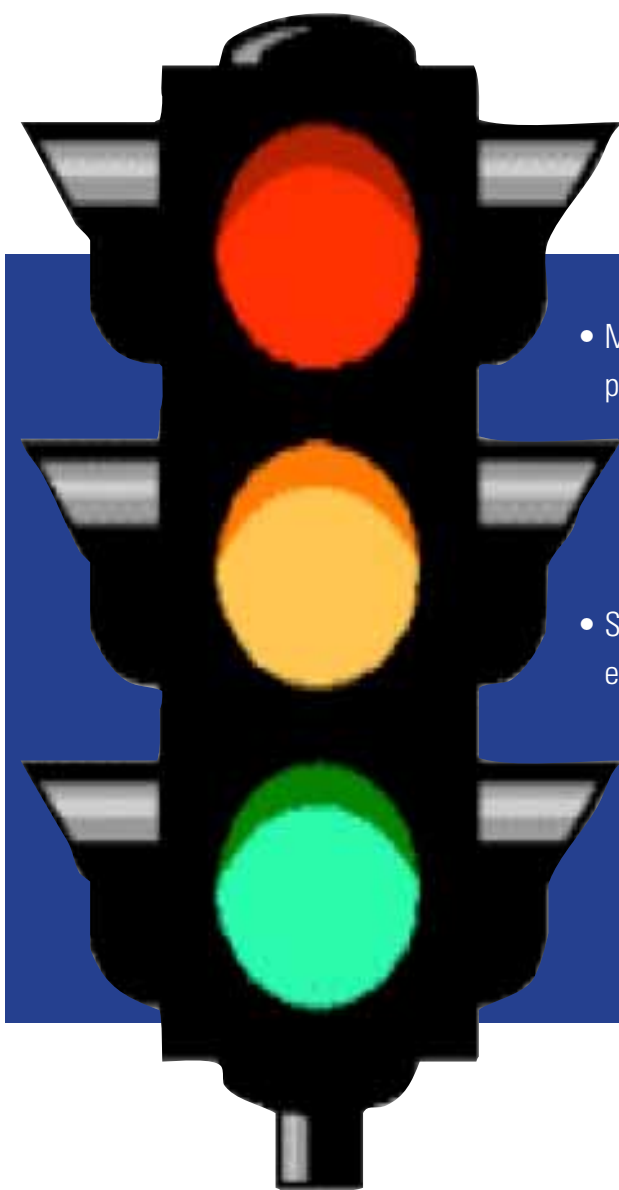
*Una macro valutazione gratuita
del livello di sicurezza digitale
del tuo sistema informatico,
compilando l'anonimo
questionario OAD 2020*

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/> il 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. E' 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. E' 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. ❖

ENAC, GARMIN, TWITTER, GLI ATTACCHI INFORMATICI NON FINISCONO MAI

I recenti attacchi informatici, con tecniche che vanno dal social engineering al ransomware al vishing, mostrano le falle alla sicurezza delle aziende

di Gaetano Di Blasio

Sono sempre più frequenti le notizie relative alla violazione dei dati e, più in generale, della sicurezza informatica.

Ovviamente l'attacco recente che ha ottenuto l'attenzione più alta da parte dei media è stato quello che ha coinvolto Twitter. Certamente da considerare grave non tanto per la cifra rubata in bit coin, circa centoventimila dollari, quanto per le ripercussioni che potrebbero sorgere a seguito della compromissione di numerosi account del noto social network, fra i quali, secondo alcune voci, quelli di Barack Obama, Joe Biden, Elon Musk nonché quelli di aziende quali Apple e Uber.

Come accennato, oltre al rischio che venissero lanciate campagne di fake news, gli account sono stati usati per una maxi truffa, cominciata con un attacco di social engineering indirizzati ai dipendenti di Twitter. Ancora una volta c'è da registrare una falla nelle politiche aziendali (per alcuni il sospetto è che ci sia stato un impiegato infedele). Gli account compromessi sono poi stati usati per attivare una truffa destinata rubare criptovalute

rapidamente: usando account compromessi di grandi scambiatori di criptovalute, veniva promesso che sarebbe stata raddoppiata la cifra che fosse stata donata a una organizzazione "benefica", per la ripresa: "cryptoforhealth", tanto per sfruttare ancora una volta il Covid-19. Ovviamente il sito su cui si sono appoggiati i cyber criminali, era fittizio e i bitcoin sono presto spariti.

La cifra rubata è stata relativamente bassa poiché l'attacco è durato durato poco. Infatti Twitter lo ha prontamente bloccato e avrebbe recuperato gli account interessati, stando ai portavoce dell'azienda. Questi stessi hanno dichiarato che la tecnica usata. Almeno a livello iniziale, appartiene alla categoria del social engineering. Con ogni probabilità una mail di spear phishing.

Secondo David Gubiani di Checkpoint Software Technology, potrebbe trattarsi di Vishing, poiché sono state rilevate campagne che utilizzavano tale strumento.

Gubiani afferma inoltre che non sia la prima volta che la privacy degli utenti della piattaforma social viene compromessa dai suoi collaboratori, né è la prima volta che i collaboratori di Twitter sono responsabili della divulgazione di dati sensibili.

L'account del CEO di Twitter Jack Dorsey è stato compromesso alcuni mesi fa dopo che il suo numero di telefono è stato acquisito in un attacco di scambio di SIM. L'anno scorso, due dipendenti sono stati accusati di aver abusato del loro

accesso alle risorse interne di Twitter e di aver aiutato l'Arabia Saudita a spiare i dissidenti residenti all'estero, sostiene ancora l'esperto.

L'attacco all'italiana Enac

Riguardandoci da vicino, riteniamo importante parlare dell'attacco subito dall'ENAC (Ente Nazionale per l'Aviazione Civile).

L'attacco, secondo quanto ci ha rilevato Mariana Pereira, Director of Email Security Products di Darktrace avrebbe reso inaccessibili alcune informazioni contenute nei sistemi dell'Ente, non sono stati sottratti dati. I sistemi di backup hanno svolto



il loro lavoro e non ci sono stati problemi in termini di violazioni, ma i tempi di ripristino sono stati lenti, il sito è rimasto bloccato per almeno 5 giorni e non è chiaro se ciò ha avuto altre ripercussioni sulle attività core. Evidentemente non è un caso che poco tempo fa l'Enac abbia presentato un sistema di pilotaggio remoto degli aerei all'avanguardia.

Presso Darktrace sospettano si tratti di un attacco ransomware e sottolineano come, in generale, queste minacce portano dei rischi per le aziende. Banalmente nel suddetto caso, un potenziale impatto è relativo all'impossibilità di accedere ai dati di chi ha preso un volo aereo da o verso il Paese evidenziano in Darktrace che ciò potrebbe ripercuotersi negativamente su indagini di polizia e sulla protezione della salute, proprio nel momento in cui le principali compagnie di volo e l'industria del turismo stessa sta riprendendo le attività.



Il blackout di Garmin

I portavoci di Garmin International hanno comunicato che il proprio sistema informatico è stato vittima di un attacco. Non è stato spiegato il dettaglio di quanto accaduto, ma con ogni probabilità si è trattato di un ransomware. I responsabili ammettono che alcuni server sono stati interessati, perciò molti dei servizi online dell'azienda sono stati immediatamente interrotti, tra cui le funzioni del sito web, l'assistenza clienti, le applicazioni rivolte ai clienti e le comunicazioni interne.

I tecnici Garmin, affermano in azienda, valutata la natura dell'attacco, hanno immediatamente attivato le procedure di risanamento dei propri sistemi informatici. Mentre scriviamo non sono stati comunicati da parte dell'azienda informazioni tali da poter confermare o escludere che i dati degli utenti, incluse

le informazioni sui pagamenti di Garmin Pay, siano stati consultati, persi o rubati. Inoltre, si precisa che la funzionalità dei prodotti tuttavia viene affermato che Garmin non è stata compromessa, fatta eccezione della possibilità di caricare e condividere i normali servizi online su Garmin Connect.

Lentamente le attività saranno tutte ripristinate, secondo quanto comunicato.

I server sono in fase di ripristino e l'azienda conta di tornare al normale funzionamento nei prossimi giorni: da una prima analisi i tecnici al lavoro non si aspettano alcun impatto negativo sulle consuete operazioni online. Tuttavia, si potranno verificare alcuni ritardi nelle risposte agli utenti dovuti alla riattivazione delle normali funzioni; l'obiettivo è quello di gestire nel minor tempo possibile eventuali richieste giunte nelle ultime ore.

L'ufficio stampa di Garmin ha comunicato che l'azienda "è consapevole del disagio arrecato agli utenti durante il blackout dei propri server e conferma che sta lavorando a pieno regime per ristabilire la normale funzionalità, ringraziando in particolare modo i milioni di appassionati per la pazienza dimostrata in queste ore"

Denis Legezo, senior security researcher di Kaspersky azzarda un'ipotesi sull'accaduto: «Ufficialmente, l'azienda ha commentato solo il "blackout" e l'"indagine" senza ulteriori dettagli sul caso che sono, invece, arrivati grazie alle foto dei dipendenti e ad altre fonti. Queste informazioni hanno dimostrato che l'incidente è il risultato di



un attacco cryptolocker e che il malware è noto come WastedLocker. L'attacco ha impedito ai clienti dell'azienda di accedere ai dati relativi alla loro attività fisica così come ai piloti di ottenere gli aggiornamenti delle mappe. Sono state colpite anche alcune linee di produzione in Asia».

Su un piano più tecnico, Legezo aggiunge; «Tecnicamente parlando, WastedLocker è un ransomware mirato, il che significa che gli attaccanti selezionano le imprese da prendere di mira e non puntano ad utenti qualsiasi. Questo non è l'unico ransomware ad essere utilizzato secondo queste modalità. Uno schema simile è quello utilizzato da Maze e da altre famiglie di ransomware. Gli algoritmi di encryption utilizzati non sono diversi da altri ransomware: moderni e forti. I creatori del ransomware aggiungono il nome della società vittima nei messaggi di riscatto. Si tratta di messaggi con informazioni su come contattare i criminali attraverso servizi di posta elettronica sicuri e simili. È quindi abbastanza chiaro che i criminali conoscono perfettamente la loro vittima. Nel caso di WastedLocker, tuttavia, fino a questo momento non abbiamo rilevato nulla a parte il criptaggio e la richiesta di pagamento di un riscatto».



CLOUD E SICUREZZA NON SEMPRE VANNO D'ACCORDO

Il 70% delle aziende ha subito attacchi nel corso dell'ultimo anno. Lo evidenzia la nuova ricerca condotta dagli esperti di cybersecurity di Sophos

di Giuseppe Saccardi

Secondo una recente ricerca svolta da Sophos, The State of Cloud Security 2020, quasi i tre quarti delle aziende (70%) ha subito un incidente di sicurezza che ha colpito il cloud nel corso dell'ultimo anno. All'origine di questo preoccupante fenomeno gli attacchi ransomware e malware (50%), l'esposizione dei dati aziendali (29%), gli account compromessi (25%) e il cryptojacking (17%).

Inoltre, le aziende caratterizzate da ambienti multi-cloud hanno il 50% di possibilità in più di essere esposte a rischi informatici di quelle che si avvalgono di un solo cloud.

In questo quadro a tinte fosche, l'Europa, osserva Sophos, risulta l'area geografica meno a rischio e ciò sembra confermare la validità e l'efficacia della normativa GDPR. Ad aver subito il maggior numero di attacchi a livello cloud è invece l'India, che con il 93% di aziende colpite nel corso dell'ultimo anno rappresenta il dato più negativo.

«Il recente sensibile incremento del ricorso al lavoro da remoto ha fornito ai cybercriminali l'occasione ideale per tentare di neutralizzare le infrastrutture



cloud strategiche ed è preoccupante che molte aziende continuino a sottovalutare l'importanza del mettere al sicuro i dati in cloud e i workload. La sicurezza del cloud è una responsabilità condivisa e le aziende devono monitorare e gestire con estrema attenzione gli ambienti in cloud al fine di essere sempre un passo avanti rispetto agli intenti dei cybercriminali» spiega Chester Wisniewski, principal research scientist di Sophos.

L'esposizione accidentale dei dati resta una vera piaga aziendale e la scorretta configurazione del cloud è all'origine del 66% degli attacchi.

Gli errori di configurazione rappresentano ancora il canale di veicolazione principale per gli incidenti di sicurezza e sono ancora troppo diffusi se si considera la complessità insita nella gestione del cloud. Un altro aspetto inquietante emerso dalla ricerca di Sophos riguarda i furti delle credenziali di accesso al cloud provider: il 33% delle aziende ha infatti



dichiarato che è così che i cybercriminali hanno avuto accesso.

Ciò nonostante, solo un quarto delle aziende ritiene che gestire gli accessi agli account cloud sia una preoccupazione prioritaria.

I dati emersi da Sophos Cloud Optix (uno strumento che offre alle aziende funzionalità di analisi e visibilità ininterrotta necessarie per identificare, rispondere e prevenire le lacune di sicurezza e conformità che espongono i sistemi ai rischi) ha rivelato poi che il 91% degli account gode di privilegi di accesso e gestione non necessari e il 98% ha disattivato l'autenticazione multi-fattore sugli account dei provider del servizio cloud.

Lo scenario italiano

Tra il campione di 26 Paesi coinvolti in questa ricerca, l'Italia è quello ad aver registrato la percentuale più bassa di incidenti di sicurezza nel public cloud nel

corso dell'ultimo anno: il 45% degli intervistati ha infatti confermato di aver dovuto far fronte a un incidente di sicurezza in tale ambito, contro il 75% del campione francese e il 61% di quello tedesco. Nonostante questo dato in parte rassicurante, ben il 97% degli intervistati italiani ha ammesso di essere preoccupato dai potenziali rischi in termini di sicurezza informatica quando si parla di Cloud.

All'origine della maggior parte degli incidenti di sicurezza (ben l'81%) vi è la configurazione scorretta del cloud che apre la porta agli attacchi.

Piuttosto contenuto il dato che riguarda invece il furto delle credenziali, che è la causa del solo 17% dei casi di attacchi al cloud.

Cresce la consapevolezza dei rischi nel cloud

Nonostante dalla ricerca emergano molti dati ancora sconfortanti, va altresì segnalato che quasi tutti gli intervistati (il 98%) hanno ammesso di essere preoccupati per il loro attuale livello di sicurezza in-the-cloud, il che dimostra che si è raggiunta una maggiore consapevolezza dell'importanza di proteggere in modo adeguato questo specifico ambito dell'infrastruttura aziendale.

Il furto di dati è naturalmente in cima alla lista dei problemi di sicurezza per quasi la metà degli intervistati (44%); l'identificazione e la necessità di rispondere tempestivamente agli incidenti di sicurezza si posizionano secondo posto per il 41% degli intervistati.

Tuttavia, a conferma che ci sia ancora molta strada da fare, va segnalato che ancora oggi solo un intervistato su quattro considera la mancanza di competenze dello staff aziendale come una preoccupazione prioritaria. ❖

PIÙ ATTENZIONE ALLA CYBERSECURITY DEI LAVORATORI DA REMOTO

Trend Micro evidenzia che in Italia cresce la consapevolezza dei rischi anche se i comportamenti pericolosi rimangono molti, soprattutto per dark web e siti hot

di Giuseppe Saccardi

Durante il lockdown, il 73% degli italiani che ha lavorato da remoto ha sviluppato una maggior consapevolezza nei confronti della cybersecurity, ma i comportamenti a rischio sono ancora molti. Il dato emerge dall'ultima ricerca Trend Micro dal titolo Head in the Clouds.

La ricerca è stata commissionata da Trend Micro e condotta da Sapio Research a maggio 2020 e ha coinvolto 13.200 lavoratori da remoto in 27 Paesi. In Italia il campione è stato di 506 persone dipendenti presso aziende di diverse dimensioni e industry.

Lo studio aveva l'obiettivo di approfondire l'attitudine dei lavoratori da remoto nei confronti delle policy aziendali IT e di cybersecurity e ha rivelato che il livello di security oggi è alto più che mai, con l'88% dei dipendenti italiani (85% Global) che dichiara di osservare attentamente le istruzioni del Team IT e l'86% (81% Global) d'accordo nell'affermare che la sicurezza della propria azienda è parte integrante delle responsabilità di ognuno. Inoltre, il 64% (64% Global) riconosce che l'utilizzo di applicazioni non

ufficiali sui dispositivi aziendali costituisce un rischio. Purtroppo, riconoscere i rischi non sempre favorisce comportamenti responsabili. Come dire che dal dire al fare c'è di mezzo il mare. Ad esempio:

- Il 51% (56% Global) dei dipendenti ammette di utilizzare applicazioni non ufficiali sui dispositivi aziendali e il 34% (66% Global) custodisce dati corporate in queste applicazioni
- il 74% (80% Global) confessa di utilizzare il



computer aziendale per navigare a scopi privati, ma il 79% (36% Global) ha impostato delle restrizioni ai siti che possono essere visitati

- Il 37% (39% Global) afferma di accedere spesso a dati aziendali da un dispositivo personale, violando le policy di sicurezza corporate
- L'11% (8% Global) ammette di accedere a siti pornografici attraverso il PC aziendale e il 5% (7% Global) al dark web

- Il 21% consente l'accesso al dispositivo aziendale ad altre persone non autorizzate, come il partner (69%), gli amici o altri familiari (31%) e i bambini (21%)

Anche la produttività ha ancora per molti utenti la meglio sulla protezione. Il 28% (34% Global) è d'accordo nel non dare importanza se l'applicazione utilizzata è consentita dall'IT oppure no, l'obiettivo è svolgere il lavoro.

Inoltre, il 28% (29% Global) pensa di poter utilizzare un'applicazione non lavorativa nel momento in cui la soluzione fornita dall'azienda non sia ottimale.

La Dottoressa Linda K. Kaye, Cyber Psicologa Accademica all'Università Edge Hill spiega "I lavoratori sono molto diversi tra di loro e ci sono molti aspetti da considerare e che influenzano il comportamento, come i valori, le responsabilità aziendali e la personalità".

Quello che ciò implica è che le aziende devono considerare queste differenze nel momento in cui effettuano corsi di formazione sulla cybersecurity con l'obiettivo di raggiungere una maggiore efficacia.

«È davvero incoraggiante vedere quante persone prendono seriamente i consigli del team IT e capiscono che la protezione della propria azienda sia anche una responsabilità individuale, anche se verrebbe da chiedersi perché gli altri non lo fanno - ha affermato Lisa Dolcini, Head of Marketing di Trend Micro Italia -. Le criticità sembrano esserci quando le consapevolezza sulla cybersecurity devono tradursi in comportamenti concreti. Le aziende devono tenere ben presenti le differenze all'interno della propria forza lavoro e insistere sulla formazione e sulla consapevolezza, in un momento in cui la cybersecurity è finalmente riconosciuta dai dipendenti come fondamentale».



IL MALWARE CRITTOGRAFATO È INVISIBILE SENZA L'ISPEZIONE HTTPS

Un Report di WatchGuard Technologies evidenzia il pericolo del malware crittografato e dà dettagli sull'impatto che la pandemia ha avuto sulla sicurezza

di Giuseppe Saccardi

WatchGuard Technologies ha rilasciato l'Internet Security Report riferito al Q1 2020. Include dati sulla percentuale di malware che viene distribuito attraverso connessioni HTTPS crittografate.

La threat intelligence realizzata mostra che il 67% di tutto il malware di Q1 è stato diffuso tramite HTTPS, pertanto le organizzazioni prive di soluzioni di sicurezza in grado di ispezionare il traffico crittografato non riusciranno a individuare i due terzi delle minacce in arrivo.

Inoltre, il 72% del malware crittografato è stato classificato come zero day, il che significa che non esiste alcuna firma antivirus per bloccarlo e che è in grado, quindi, di bypassare le soluzioni di protezione basate sulla firma.

I risultati, osserva la società, confermano che l'ispezione HTTPS e le soluzioni avanzate di rilevamento e risposta alle minacce basate sul comportamento sono requisiti fondamentali per ogni organizzazione attenta alla sicurezza.

Il rapporto include anche una sezione speciale che

illustra in dettaglio l'impatto del COVID-19 sul panorama delle minacce.

«Alcune organizzazioni sono riluttanti a impostare l'ispezione HTTPS a causa del lavoro aggiuntivo richiesto, ma i nostri dati sulle minacce mostrano

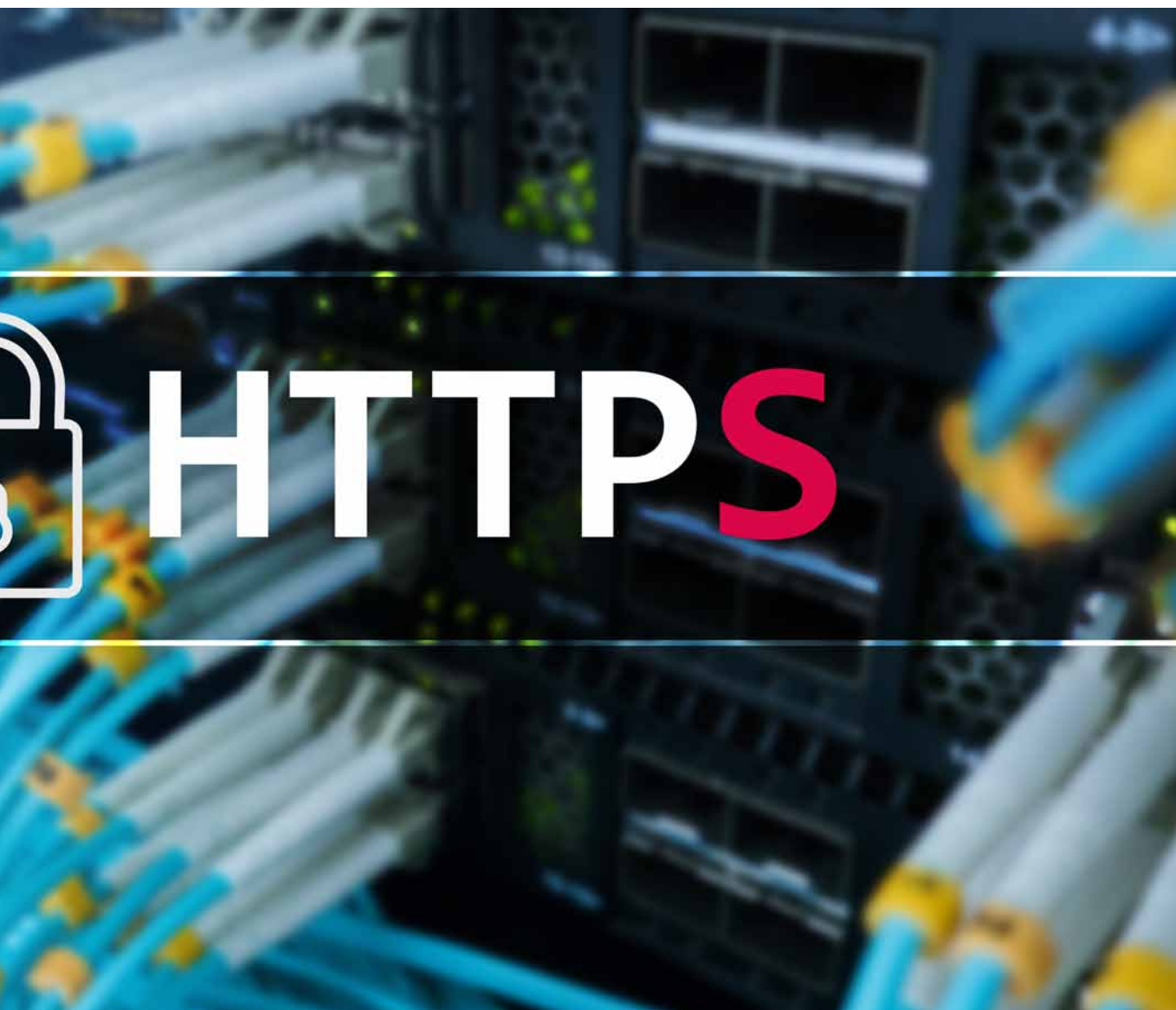


chiaramente che la maggior parte del malware viene distribuito attraverso connessioni crittografate e lasciare che il traffico non venga ispezionato non è più un'opzione possibile - ha affermato Corey Nachreiner, chief technology officer di WatchGuard -. Poiché il malware continua a diventare più avanzato ed evasivo, l'unico approccio per la difesa è l'implementazione di una serie di servizi di sicurezza a più livelli, inclusi metodi avanzati di rilevamento delle minacce e ispezione HTTPS».

L'Internet Security Report si basa sui dati in forma

anonima provenienti dai Firebox Feed di appliance WatchGuard attive i cui proprietari hanno acconsentito alla condivisione dei dati per supportare gli sforzi di ricerca del Threat Lab di WatchGuard.

Il report completo include anche le migliori pratiche difensive che le organizzazioni possono utilizzare per proteggersi nel panorama odierno delle minacce e un'analisi di come la pandemia di COVID-19 e il conseguente aumento dell'home working abbiano influenzato il panorama della sicurezza informatica. ❖

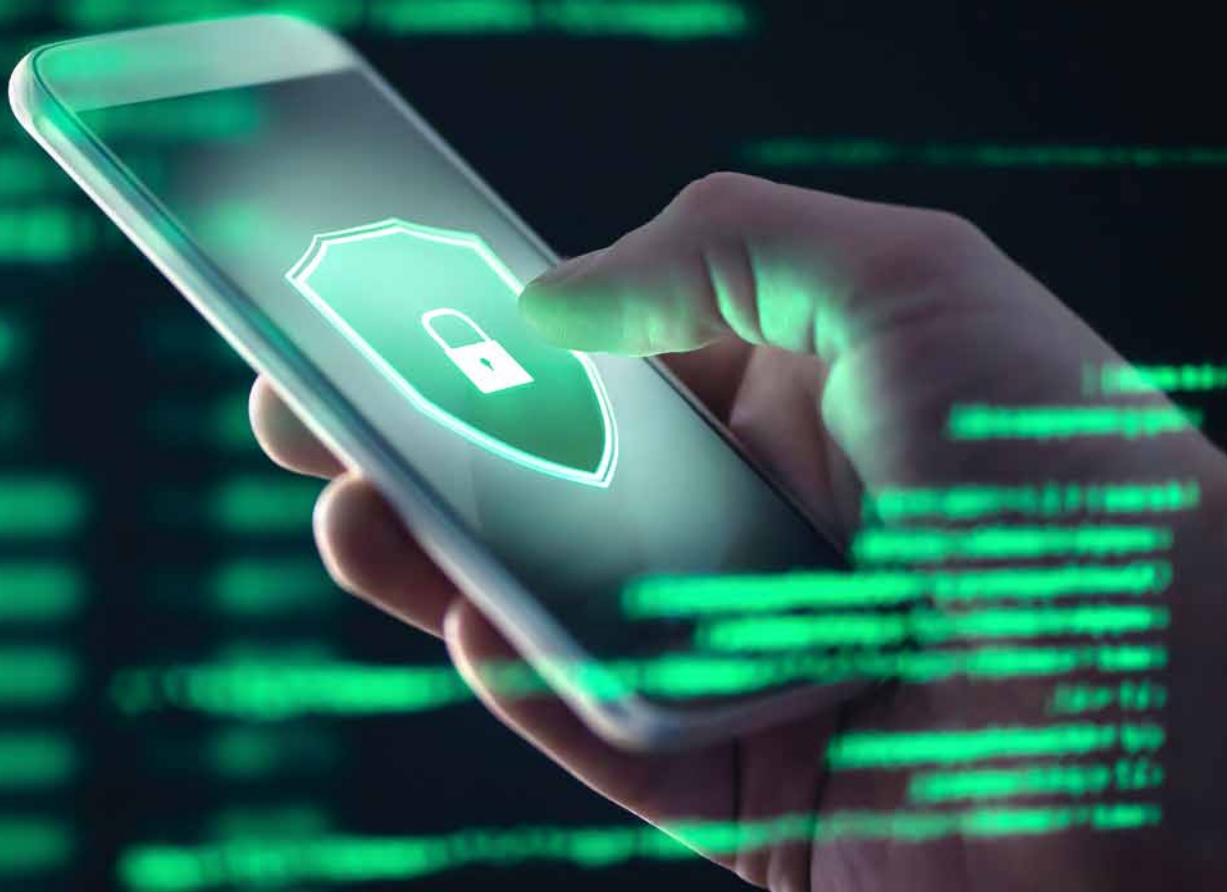


SEMPLIFICARE LA GESTIONE DELLA SICUREZZA AZIENDALE

Kaspersky Lab Italia spiega come in questo periodo di emergenza sia importante aumentare l'attenzione verso la gestione della sicurezza, con particolare attenzione agli endpoint

di Gaetano Di Blasio

Morten Lehn, General Manager Kaspersky Lab Italia, evidenzia come questo periodo, segnato dalla pandemia, abbia portato nuovi comportamenti online con una crescita elevatissima in termini di problematiche per la sicurezza. Questo soprattutto sul fronte degli end point, che vede la società fondata da Eugeny Kaspersky in prima linea. Lehn, in particolare, evidenzia la stabilità delle





Morten Lehn, General Manager Kaspersky Lab Italia

soluzioni e la crescita dei partner che forniscono servizi per aiutare le imprese a semplificare la gestione della security. Questo in un momento in cui sale nelle aziende la consapevolezza di quanto sia importante la sicurezza.

Gianpaolo Dadola, senior Security Researcher del GREAT (Global Research and Analysis Team di Kaspersky, evidenzia due minacce che si contengono il primato di "minaccia del momento": il web skimming e il targeted ransomware, cresciuti rapidamente nel 2019 e tuttora un grosso problema per le imprese. Infatti hanno un impatto elevato.

Basti considerare che tali minacce sono di tipo mirato. Invece che cercare di bloccare sistemi a caso, puntano a bloccare le attività di un'impresa fermando tutti i sistemi, per poi chiedere un riscatto.

Attaccano imprese di tutte le dimensioni. Inoltre è stato alzato il costo dei riscatti e si sono aggiunti altri tipi di ricatti, attraverso la divulgazione dei dati aziendali che riescono a rubare. Qui si aprono svariati scenari dell'uso che di tali dati è possibile fare. Questi attacchi sfruttano combinazioni di tecniche, come nel caso degli APT, ma impiegando anche strumenti usati per i penetration test.

Occorre cercare le tracce e identificare i meccanismi impliciti degli attacchi. Ovviamente, partono quasi tutti da uno spear phishing .

Altro strumento usato è l'attacco che parte da un endpoint "semidimenticato", sul quale si trovano password deboli. Si prosegue, quindi, con un attacco di

forza bruta che non dovrebbero essere efficaci se si usassero password forti.

Un tipo di attacco subdolo è quello che utilizza gli strumenti degli MSP (Managed Service Provider), molti dei quali. Inoltre, hanno mostrato una certa qual mancanza di competenze, che Dadola non commenta.

L'esperto, però, sottolinea come i cyber criminali collaborino fra loro riuscendo a creare minacce miste. I security manager devono imparare a non sottovalutare anche piccoli indizi (per esempio, sono stati rilevati malware generici che l'antivirus ha intercettato fermando il contagio, ma, all'interno erano nascoste altre minacce che si sono attivate successivamente.

A fine 2019, il numero di file malevoli identificati, secondo Kaspersky Lab, era di 24,6 milioni. Una pressione indiscutibile e in continuo cambiamento, rileva Dadola, che torna sul web skimming.

Questo esiste da tempo: si tratta di iniettare codici malevoli in vari siti, perlopiù quelli che hanno sezioni di e-commerce e più in generale quelli che

possono contenere dati carte di credito, ma anche malvertising. Corrotto il sito, da lì si cerca di compromettere siti terzi.

L'obiettivo è spostare i dati, impacchettando i dati per spedirli a un server legittimo che non desti sospetti. « Addirittura c'è stato un caso in cui i dati sono stati spediti su un server legittimo di un sito Google Drive, superando in tal modo tecnologie di detection. I dati erano "nascosti" fra i metadati di immagini.

La risposta di EDR Optimun

Fabio Sammartino, Head of Pre Sales in Kaspersky Italia, riprende lo scenario descritto da Dadola, addentrandosi nell'ambito della soluzione fornita dalla azienda d'origine russa Kaspersky Integrated Endpoint Security, che combina Kaspersky EDR Optimun e Kaspersky Sandbox, fornendo funzionalità di incident response anche per le medie e grandi imprese. Entrando in dettaglio, Kaspersky Endpoint Security for Business si integra con Cloud Management Console, Kaspersky Endpoint Detection and Response Optimun (EDR e Kaspersky Sandbox. Un nuovo EDR personalizzato anche per le organizzazioni con minori competenze che consentirà agli specialisti di sicurezza IT di ottenere visibilità e insight istantanei sugli incidenti, insieme a indagini immediate e opzioni di risposta automatizzate.

Più precisamente, Kaspersky EDR Optimun è stato specificamente progettato per le aziende che vogliono avere una visione d'insieme sugli incidenti di

sicurezza e sulla capacità dell'azienda di reagire agli attacchi, senza però sovraccaricare ulteriormente il proprio team e le proprie risorse, evidenzia Sammartino. Inoltre la soluzione aggiunge la possibilità di una visibilità immediata sulle minacce rilevate da Kaspersky Endpoint Security for Business, fornendo uno scenario completo di tutte le attività maligne: dati più dettagliati sugli alert e visibilità sul percorso di diffusione degli attacchi.

Le funzioni Sandbox si attivano per controllare il comportamento di un file: questo viene analizzato e, eventualmente, passato all'analisi parte di Kaspersky EDR Optimun.

Maggiore protezione per gli endpoint grazie al cloud

Il nuovo Kaspersky Endpoint Security rafforza la protezione degli endpoint con sistema operativo Linux, evidenzia Sammartino, sottolineando che i componenti di protezione contro le minacce rivolte alla rete e al Web garantiscono che il traffico in entrata e in uscita è privo minacce.

Inoltre, Integrated Endpoint Security fornisce una gestione semplificata, grazie alla console di gestione Kaspersky Security Center, ora disponibile anche che on-premise.

Il vantaggio, spiegano presso la società, consiste in una implementazione più rapida con minori costi, ma soprattutto con la garanzia che gli aggiornamenti e le altre operazioni di manutenzione saranno gestiti da Kaspersky.



SICUREZZA E AFFIDABILITÀ IN AZIENDA CON LE SOLUZIONI PRAIM

P.E. Labellers ha offerto con Prait ai collaboratori la possibilità di lavorare da remoto, in autonomia e mantenendo la sicurezza dei sistemi informativi

di Giuseppe Saccardi

Prait, azienda che sviluppa soluzioni software per la creazione e gestione di postazioni di lavoro evolute e soluzioni hardware Thin & Zero Client, ha supportato P.E. Labellers, multinazionale italiana attiva nel settore delle macchine etichettatrici automatiche, con una soluzione rivelatasi la più idonea

allo svolgimento delle attività dei propri dipendenti anche da remoto.

P.E. Labellers è un gruppo nato nel 1974; che da allora è cresciuto sino a raggiungere le attuali dimensioni globali. È composto da 8 aziende distribuite tra Italia, Stati Uniti e Brasile, ed è a sua volta parte del gruppo multinazionale statunitense Pro Mach. L'azienda si è specializzata nel tempo nella creazione di soluzioni di etichettatura di alto livello, tanto da essersi conquistata la fiducia dei più grandi gruppi aziendali globali, dei maggiori OEM così come di aziende di dimensioni più contenute e con esigenze produttive a loro volta diverse.

P.E. è legata anche alle filiere produttive delle industrie alimentari, vitivinicole, casearie, farmaceutiche, chimiche e cosmetiche.

Le macchine P.E. installate nel mondo ad oggi sono circa 10.000 e i servizi professionali di assistenza e manutenzione vengono erogati in tutto il mondo, contando su una forza di oltre 90 profili esperti che

supportano i clienti e oltre 480

dipendenti che operano ogni giorno con standard qualitativi superiori, in ogni dipartimento di ciascuna sede nel mondo.

È in questo ampio e complesso scenario, e conseguentemente all'espansione del proprio business, che P.E. Labellers aveva





sede P.E. Labellers

la necessità di ampliare il parco installato e gestirlo nella maniera più semplice e centralizzata possibile, con soluzioni sia per il lavoro in azienda che da remoto e rispondendo anche ai particolari requisiti tecnici propri delle peculiari attività aziendali.

L'obiettivo, nell'ottica di un miglioramento continuo, a tutti i livelli e dipartimenti, era di procedere con l'implementazione di dispositivi con ottime performance grafiche e di calcolo, il mantenimento della gestione centralizzata e la possibilità di effettuare assistenza remota sulle postazioni, assicurando un livello di efficienza adeguato alla necessità di garantire continuità di servizio.

A questa esigenza hanno risposto Praim e l'azienda informatica altoatesina ACS Data System, legati da una collaborazione di lunga data, con una prima dotazione, nel 2019, di 30 sistemi software Praim-based con il sistema operativo Praim ThinOX4PC messi a disposizione dei dipendenti di vari dipartimenti aziendali, e nel 2020 con la fornitura di altri 14 sistemi, riscontrando una generale soddisfazione da parte di tutti i collaboratori.

«L'implementazione delle nuove postazioni è stata estremamente semplice: dopo aver installato ThinOX4PC sui dispositivi, gli stessi sono stati collegati alla rete (wired o wi-fi) e, tramite la console di gestione degli endpoint Praim ThinMan, sono stati distribuiti tutti gli aggiornamenti e le impostazioni necessari all'accesso all'infrastruttura Terminal Server o VDI», ha commentato Jacopo Bruni, Marketing

Manager di Praim.

Tutti gli ambienti sono stati trasformati in postazioni di lavoro che, ha osservato l'a-

zienda, si sono rivelati molto efficaci. La necessità di fornire hardware dalle performance adeguate, difficilmente soddisfacibile con solo hardware standard Thin Client ha portato Praim a suggerire una configurazione mista di hardware standard PC sul quale installare il sistema operativo Praim ThinOX4PC.

«I vantaggi ottenuti dall'aver scelto questa soluzione tecnologica sono stati molteplici - ha spiegato Andrea Sanfelici, IT Manager P.E. Labellers -, abbiamo potuto assecondare le necessità di operatori finali con esigenze diverse, a cui viene data la soluzione chiavi in mano per poter lavorare da casa senza veder alterata la propria operatività quotidiana, tanto nella progettazione 3D quanto nell'accesso ai server. Allo stesso tempo, la soluzione viene incontro anche alle esigenze dell'amministratore di rete. Per noi tutelare e mantenere la sicurezza dei sistemi informativi è una priorità imprescindibile, estesa all'intero gruppo P.E. Labellers, ramificato in otto aziende diverse dislocate sul territorio. Il dispositivo con software Praim a bordo garantisce la protezione e l'inalterabilità degli applicativi installati, che risiedono sui server aziendali e quindi governati centralmente. Una delle sfide del nostro lavoro sta proprio nel fornire alle nostre persone soluzioni tanto affidabili quanto user friendly, la cui complessità tecnologica è erogata in modo totalmente trasparente. Centrando l'obiettivo sicurezza.»

