CONFINDUSTRIA
Varese

IL DECALOGO PER LA **SICUREZZA INFORMATICA NELLE IMPRESE**

PUNTO**ZERO** | 20**22**

GUIDA ALLA LETTURA

Il rischio informatico è recentemente balzato ai primi posti nelle classifiche delle preoccupazioni percepite dalle imprese di ogni dimensione in ogni parte del mondo (fonte Allianz AGCS).
La cronaca di questi mesi ha messo in evidenza quanto siano pericolosi gli attacchi mirati ed organizzati contro imprese ed enti pubblici.
La verità è che per quanto possano essere inquietanti questo tipo di aggressioni e per quanto sia auspicabile che un'impresa si prepari ad un'eventualità così grave, statisticamente si tratta solo della cosiddetta "punta dell'iceberg".
Il problema della Sicurezza è certamente vasto e complesso. L'informatizzazione sempre più pervasiva dei processi aziendali aumenta di fatto i rischi di interruzione critica dell'attività in conseguenza di incidenti. Nessun sistema informatico è sicuro o affidabile al 100%. La protezione fisica degli strumenti informatici e degli ambienti che li ospitano, la tutela di dati e sistemi da violazioni o errori umani, la conformità a leggi e regolamenti come il GDPR sono solo alcuni degli aspetti che ogni giorno le imprese si trovano ad affrontare.
Tuttavia, soprattutto nelle imprese meno strutturate, dove, per ragioni dimensionali o di budget, non è possibile avvalersi di professionalità specifiche, esiste il rischio di rimandare la gestione del problema a tempi migliori che però non arrivano mai, oppure di considerare la questione troppo complessa per essere affrontata in modo sistematico e organico.
In questi contesti si tende spesso a stratificare soluzioni tecnologiche (antivirus, firewall, antispam ecc.) che sono certamente utili se non indispensabili, ma talvolta insufficienti a garantire un adeguato livello di protezione dei dati e, in ultima analisi, della continuità dell'attività di impresa.
Serve dunque un approccio di ampio respiro, in grado di tenere sotto controllo diversi aspetti. Per primo il fattore umano: è noto ormai che la maggior parte degli incidenti di sicurezza è causato da comportamenti errati, spesso per mancanza di formazione o addirittura di informazioni.
Questa breve guida, nata per iniziativa del Gruppo merceologico "Terziario Avanzato" di Confindustria Varese, in stretta collaborazione con i Sistemi Informativi dell'Associazione, non ha certo la pretesa di essere totalmente esaustiva, ma piuttosto vuole essere un'occasione di riflessione tramite un percorso graduale di avvicinamento alla problematica della protezione dei dati.
Le parti fondamentali che costituiscono la guida sono tre.
Nella **prima parte** il lettore troverà una trattazione in tono divulgativo e di facile fruizione degli argomenti fondamentali per conoscere meglio la pur complessa tematica della Sicurezza Informatica.
La **seconda parte** rappresenta il cuore del progetto di comunicazione: dieci punti da "ponderare" attentamente che possono ispirare un metodo di gestione e miglioramento continuo in azienda. Un percorso a tappe pensato soprattutto per le Piccole e Medie imprese, per non lasciare nulla al caso.
La **terza parte** è il "Vocabolario della Sicurezza". Si tratta di un tentativo di spiegare con parole semplici e comprensibili anche ai non addetti ai lavori i termini più ricorrenti nell'articolato mondo della Sicurezza Informatica.
Infine, nel momento in cui l'impresa vorrà, anche grazie alla spinta di questa guida, "passare all'azione", saranno necessarie consulenze e competenze professionali adeguate alle singole esigenze. Per questo, nelle ultime pagine il lettore troverà il riferimento ad una pagina Web del Sito Internet di Confindustria Varese (www.confindustriavarese.it), attraverso la quale sarà possibile consultare una tabella che rappresenta quali siano le competenze sul territorio e quelle segnalate direttamente dalle imprese del "Terziario Avanzato" associate a Confindustria Varese. In questo modo, ogni singola azienda, in base alle proprie necessità, potrà autonomamente decidere a chi rivolgersi per ottenere consulenza o servizi.

Buona lettura, dunque, con l'auspicio che questa guida possa contribuire, almeno in parte, a rendere le imprese più sensibili ai temi della Sicurezza Informatica.

SOMMARIO

LO SCENARIO


GDPR

INTEGRITÀ • DISPONIBILITÀ • RISERVATEZZA

Non esiste una formula certa e condivisa per definire la Sicurezza Informatica. Forse perché la Sicurezza Informatica, come «concetto assoluto», non esiste. Nessun sistema può essere definito come completamente sicuro e non si può acquistare la Sicurezza come un prodotto «da scaffale». È però possibile identificare e rendere operativi un insieme di processi, comportamenti, strumenti tecnologici e competenze, tutti finalizzati alla protezione di INTEGRITÀ, DISPONIBILITÀ e RISERVATEZZA dei dati, mitigando gli effetti delle varie fattispecie di rischio che si possono presentare ogni giorno nella vita di un'impresa.
Si tratta, in realtà, di concetti semplici da comprendere, ma la loro declinazione pratica, in un mondo sempre più interconnesso e sempre più complesso, può trasformarsi in una vera e propria sfida.

Confindustria Varese si pone l'obiettivo di rendere questa sfida affrontabile, partendo dalle basi, da un «punto zero».
Vogliamo iniziare a creare in azienda la cultura della sicurezza, un passo alla volta.

Abbiamo usato il termine «cultura» perché al primo posto negli strumenti di prevenzione dei rischi informatici c'è sempre il cosiddetto fattore di rischio umano, cioè tutti quei comportamenti, consapevoli o meno, che portano ad un aumento esponenziale delle probabilità di incorrere in un incidente con i dati. L'esempio più calzante riguarda il nostro rapporto con lo smartphone. Siamo sempre noi gli artefici di ciò che diffondiamo, di ciò che archiviamo, della custodia dell'apparecchio, della sua integrità, delle sue configurazioni. Nel momento stesso in cui commettiamo un errore, come ad esempio distruggerlo o smarrirlo senza aver previsto un backup in cloud e senza aver attivato un blocco PIN, ci troviamo in una frazione di secondo nella condizione di NON INTEGRITÀ, NON DISPONIBILITÀ e NON RISERVATEZZA.

Tornando ai concetti iniziali di INTEGRITÀ, DISPONIBILITÀ e RISERVATEZZA, vediamo nel dettaglio qual è il significato di questi tre principi chiave, conosciuti anche con l'acronimo **CIA (Confidentiality, Integrity, Availiability)** ai quali si aggiunge un ulteriore pilastro: la normativa (il GDPR per i cittadini dell'UE).

CIA (Confidentiality, Integrity, Availiability)

INTEGRITÀ
Garantire che i dati non vengano alterati da programmi, processi o personale non autorizzato. Sia a seguito di un attacco, sia per comportamenti consapevolmente o inconsapevolmente sbagliati.

DISPONIBILITÀ
Garantire che i sistemi siano funzionanti e che i dati siano utilizzabili con adeguato livello di efficienza, secondo le regole prestabilite.

RISERVATEZZA
Garantire che i dati siano accessibili solo a chi ne ha diritto in tutto il loro ciclo di vita (durante il loro utilizzo, quando vengono trasmessi o quando vengono archiviati).

Quali sono quindi gli strumenti per garantire questi tre aspetti fondamentali? Si tratta di agire su tre ulteriori ambiti, altrettanto fondamentali:
COMPETENZE, PROCESSI, TECNOLOGIE.

Vediamoli uno per uno.

Competenze

Di nuovo il «fattore umano», cioè quell'insieme di informazioni, abitudini, sensibilità che da sole sono sufficienti a ridurre sensibilmente i rischi. L'esperienza aiuta ma non si può prescindere dal ruolo centrale della formazione. Quanto più la formazione è puntuale, mirata e adeguata al contesto operativo, quanto più è efficace nel generare quel «senso critico» che aiuta a individuare le minacce quando si presentano. Certamente le competenze non saranno le stesse per tutti. Man mano che si scende in profondità verso chi governa l'infrastruttura, avremo competenze tecniche crescenti con ruoli e responsabilità definite.

Processi

Le procedure, le policy, le regole in grado di modificare o orientare comportamenti e di agire sui flussi di informazioni, aiutandone la razionalizzazione in ottica di sicurezza. La gestione dell'identità e degli accessi, le regole per la condivisione, trasmissione ed archiviazione dei dati, i requisiti di sicurezza per le applicazioni fanno parte di questa famiglia di strumenti così come le normative (il GDPR) oppure i framework di sicurezza o di certificazione come le norme ISO 27001, sempre più utilizzate in ambito internazionale o di filiere di subfornitura evolute. Prendono sempre più piede anche attività di monitoraggio del «sottobosco» del web, dove possono essere scoperte compromissioni di dati e credenziali oppure individuate volontà di attacco alla nostra impresa.

Tecnologie

L'insieme di strumenti software e hardware, in grado di prevenire, individuare o rendere inoffensiva una minaccia alla sicurezza.

YEKO PHOTO STUDIO/FREEPIK.COM

L'esempio più immediato è rappresentato dai conosciutissimi antivirus, ma le tecnologie per la sicurezza sono davvero tante e in continua evoluzione, per essere sempre al passo con le strumentazioni avanzate e sofisticate messe a disposizione dei criminali informatici da vere e proprie web company «del lato oscuro» della Rete. Sicurezza del network, del «perimetro aziendale», dei server e delle postazioni, sistemi di intelligenza artificiale finalizzate alla individuazione precoce di situazioni critiche sono solo alcuni degli ambiti in cui la tecnologia supporta la sicurezza. Oggi si parla anche di automazione della sicurezza proprio perché la complessità in alcuni ambienti professionali è talmente elevata da rendere difficile l'approccio attendista tradizionale.

FREEPIK.COM

LE PRINCIPALI MINACCE

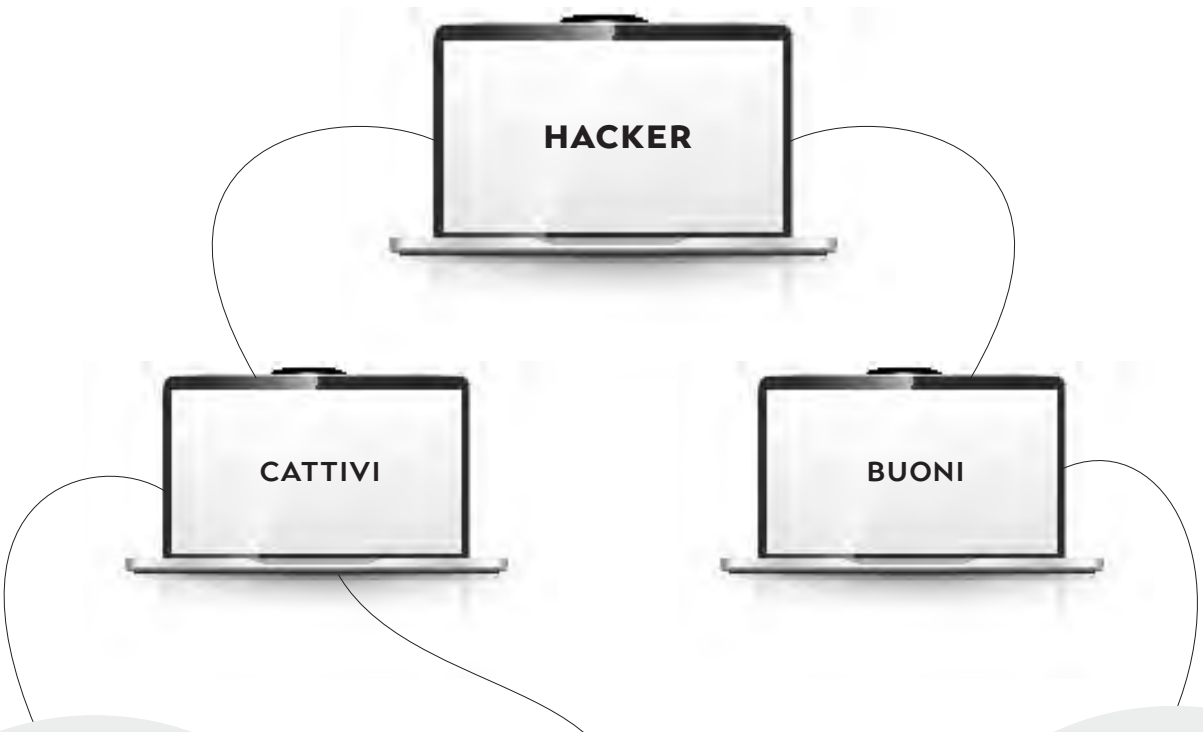
Quali sono le principali minacce alla sicurezza informatica? Ma, soprattutto, perché esistono e che finalità hanno gli attacchi?
Abbiamo già detto che la minaccia principale alla sicurezza dei dati siamo noi stessi con i nostri errori e le nostre «leggerezze», ma se ci concentriamo solo sulle attività cosiddette «malevole» messe in atto da terzi, occorre mettere in chiaro che la criminalità informatica agisce quasi esclusivamente per rubare o estorcere dati e denaro, possibilmente criptovalute.
Esistono anche attività ostili legate a motivazioni politiche etiche o religiose o comunque riconducibili ad una qualche forma di attivismo digitale, ma sono meno frequenti nell'ambito aziendale. Scordiamoci quindi l'immagine romantica dell'hacker genio «nerd felpa e cappuccio» e impariamo a considerare le violazioni a dati e sistemi come reati. Pensiamo agli attaccanti come a vere e proprie imprese criminali in grado di disporre di servizi digitali avanzati, disponibili «on demand» nei negozi online del dark web.
In alcuni casi queste vere e proprie «corporation criminali» sono in grado di mettere a rischio processi fondamentali del vivere civile e democratico, come abbiamo visto nei recenti eclatanti attacchi a infrastrutture strategiche negli Stati Uniti.

IL MERCATO DEI DATI

**I nostri dati personali fanno gola. Possono certamente essere raccolti e trattati in modo lecito e rispettoso del GDPR, oppure rimanere in una zona d'ombra secondo le diverse normative internazionali.
Ma di sicuro non c'è nulla di legale nel mercato nero dei dati personali che nel dark web è sempre più fiorente. Credenziali, dati sanitari, documenti, numeri di carta di credito, account bancari in genere ottenuti attraverso le varie e diversificate tecniche di attacco sono merce pregiata. A volte i dati frutto di effrazioni vengono messi all'asta in blocco su piattaforme specializzate. Con adeguati motori di ricerca, risulta facile per un attaccante trovare in vendita credenziali compromesse appartenenti ad una azienda che si vuole attaccare ed acquistare il dato per poche decine di dollari.
Sono anche in vendita tabelle di dati personali apparentemente innocue, ma che possono essere utilizzate per attacchi «spear phishing», un tipo di attacco fortemente personalizzato, che può trarre spunto dal contesto nel quale quel dato è stato trafugato. Ad esempio, tutti i possessori di un certo bene di consumo, oppure tutti i clienti di una certa società possono essere oggetto di e-mail malevole molto credibili e circostanziate.**

BUONI O CATTIVI?

Il termine "hacker" viene normalmente associato ad attività illecite in un immaginario di personaggi con felpe e cappuccio, cantine buie rischiarate dal bagliore di molteplici monitor su cui scorrono indecifrabili scritte. Il reale significato della parola è in realtà "persona in grado di mettere a frutto le proprie conoscenze informatiche per estendere le potenzialità di un sistema o individuarne i punti deboli per migliorarlo". Tecnicamente, quindi, i criminali informatici dovrebbero essere chiamati "cracker".
Tuttavia, nel nostro linguaggio comune, il termine hacker ha preso il sopravvento per indicare sia chi commette reati informatici sia coloro i quali, muniti di altrettanta competenza, lottano per prevenirli, lavorando in vari ambiti della ricerca o della Sicurezza Pubblica.



IMPROVVISATI/ SMANETTONI

DIPENDENTI INFEDELI

SINGOLI ATTIVISTI

ATTIVISMO ORGANIZZATO

TERRORISMO

GRUPPI CRIMINALI

SPIONAGGIO

POTENZE STRANIERE

RICERCATORI

HACKER ETICI

LOTTA AL CRIMINE E AL TERRORISMO

IL MALWARE

Per malware si intende genericamente qualunque tipo di software malevolo come ad esempio virus, spyware, trojan, cryptolocker. Nella maggior parte dei casi vengono veicolati all'azienda tramite e-mail di phishing. I più sofisticati malware penetrano le difese di una rete e poi scaricano a loro volta altri moduli dannosi, rendendo invisibile la loro attività fino al momento più opportuno.

I loro obiettivi sono generalmente:

→ **Copiare dati all'esterno che saranno poi analizzati, venduti o utilizzati per ricatto;**
→ **Bloccare accesso a dati e sistemi per ricattare l'azienda e chiedere un riscatto (ransomware);**
→ **Porre la macchina o la rete nella piena disponibilità dell'hacker che la utilizzerà in un secondo momento, ad esempio per sferrare attacchi ad ulteriori bersagli, facendo poi perdere le proprie tracce;**
→ **Sfruttare in modo silente l'infrastruttura infetta per fini illeciti privati come ad esempio il mining di criptovalute.**

N.B. *Nella maggior parte dei casi, i criminali prendono possesso di un sistema diverse settimane prima di sferrare l'attacco (mediamente sette settimane). Questo tempo serve per acquisire dati ed informazioni utili, per valutare la tipologia dell'azione malevola e calibrare eventuali richieste economiche di riscatto.*

RANSOMWARE: I CONSIGLI DEGLI ESPERTI

→ **Gli attacchi Ransomware (crittografia massiva di tutti i dati aziendali e richiesta di riscatto) rappresentano, ad oggi, una delle minacce più serie in ambito Sicurezza Informatica.**

È quindi indispensabile prevenire, ma anche prepararsi a questa eventualità con interventi di messa in sicurezza dell'infrastruttura e dei dati come vedremo nei prossimi capitoli;

→ **Non bisogna solo cautelarsi dalla compromissione dei dati, ma anche dal fatto che prima dell'attacco essi vengono generalmente copiati in massa, per rinforzare il ricatto sotto la minaccia della divulgazione.**

Bisogna valutare la crittografia dei dati critici: in caso di sottrazione o accesso non autorizzato, gli stessi saranno illeggibili per chiunque non sia in possesso delle chiavi di decrittazione;

→ **Attenzione al triplice ricatto. Oltre alla crittografia e alla minaccia di divulgazione, i criminali sferreranno degli attacchi interdittivi (DoS o DDoS) in grado di paralizzare i servizi ancora funzionanti per costringere la vittima a pagare.**

RANSOMWARE. PAGARE O NON PAGARE?

In caso di attacco ransomware l'impresa affronta una crisi gravissima. L'indisponibilità di dati e sistemi manda in stallo le attività e la situazione si aggrava di ora in ora. Può farsi strada la tentazione di risolvere tutto pagando un riscatto tutto sommato ragionevole. Ecco i motivi per cui potrebbe non essere una buona idea:

→ **Pagare un riscatto significa alimentare una organizzazione criminale e potrebbe essere illegale sotto vari punti di vista;**

→ **La disponibilità dell'azienda a cedere ad un ricatto verrà registrata e diverrà un'informazione condivisa nel mondo del crimine informatico;**

→ **Non c'è alcuna certezza di poter avere i dati originali. L'evoluzione degli assetti delle bande criminali informatiche e le contromisure messe in atto da alcuni Paesi stanno mutando lo scenario in modo repentino. L'attaccante potrebbe già essere sparito al momento del pagamento.**

IL PHISHING

Il Phishing consiste nell'invio di comunicazioni fraudolente che sembrano provenire da una fonte attendibile e conosciuta. Solitamente il veicolo del Phishing è una e-mail, ma sempre più spesso si assiste anche al cosiddetto smishing che si diffonde via sms/instant messaging. L'obiettivo è quello di impossessarsi di dati di accesso (credenziali) o dati bancari come carte di credito, PIN, oppure di installare un malware sul computer della vittima. Il 70% degli attacchi informatici ad oggi esordisce con una e-mail di phishing. Se l'attacco phishing è mirato ad una singola impresa prenderà il nome di spear phishing e presenterà caratteristiche tali da far apparire evidente una fase di studio preliminare.

Il principio su cui si basa il Phishing è detto Social Engineering. Si tratta di un insieme di tecniche sofisticate finalizzate a convincere un ignaro utente dell'autenticità ed autorevolezza del messaggio, che così sembra provenire da vertici aziendali, banche, persone ben conosciute o addirittura essere una risposta ad un nostro precedente invio.

ALCUNI ESEMPI DI PHISHING

→ Enfasi sull'azione che provoca l'infezione
→ Numero linea inesistente e italiano scorretto

TIM

Il futuro firmato Telecom Italia

Gentile pippo@tin.it,

ti informiamo che la tua fattura TIM di **luglio 2017** relativa alla linea **000849220-0387800** è stata appena emessa ed è disponibile online.

Si prega di scaricare il fattura

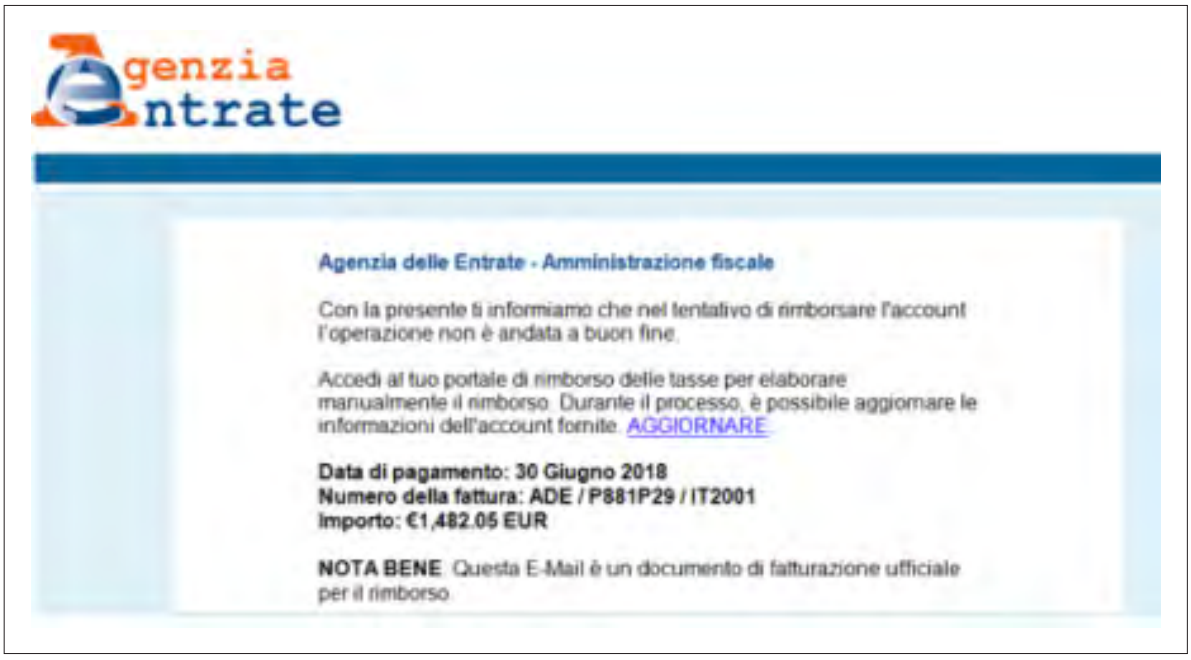
Ti ricordiamo che in MyTIM Fisso nella sezione Il mio profilo puoi richiedere di ricevere la **fattura TIM** esclusivamente online. **Risparmierai così le spese di spedizione postale.**

Ti aspettiamo presto su **www.tim.it**

Grazie

Servizio Clienti tim.it

→ Enfasi sull'azione che provoca l'infezione
→ Prospettiva allettante di incassare una discreta cifra, italiano accettabile



Agenzia Entrate

Agenzia delle Entrate - Amministrazione fiscale

Con la presente ti informiamo che nel tentativo di rimborsare l'account l'operazione non è andata a buon fine.

Accedi al tuo portale di rimborso delle tasse per elaborare manualmente il rimborso. Durante il processo, è possibile aggiornare le informazioni dell'account fornite. AGGIORNARE

Data di pagamento: 30 Giugno 2018
Numero della fattura: ADE / P881P29 / IT2001
Importo: €1,482.05 EUR

NOTA BENE Questa E-Mail è un documento di fatturazione ufficiale per il rimborso

→ Si fa leva sul timore di possibili accertamenti fiscali, ottimo italiano, errori ortografici, saluto di apertura improbabile

Agenzia Entrate

Ciao,

Si invitano tutte le persone fisiche e giuridiche a visionare e seguire con rigore Le Linee Guida fornite dall'Agenzia delle Entrate (in allegato).
E sufficiente seguire le indicazioni per evitare di essere segnalato dal sistema come un soggetto "a rischio" dopo il primo controllo basato sul c.d. "reddittometro".
Il materiale da consultare (Le Linee Guida) viene consigliato specialmente ai soggetti che utilizzano i servizi bancari finanziari (es. Internet Banking).

Nell'ambito dell'attività di controllo nei confronti delle persone fisiche e giuridiche, nel 2019 è stata data attuazione alla normativa prevista dall'art. 38, commi quarto e seguenti del D.P.R. n 600/73 e dal D.M. 24 dicembre 2018 (il cosiddetto Reddittometro).

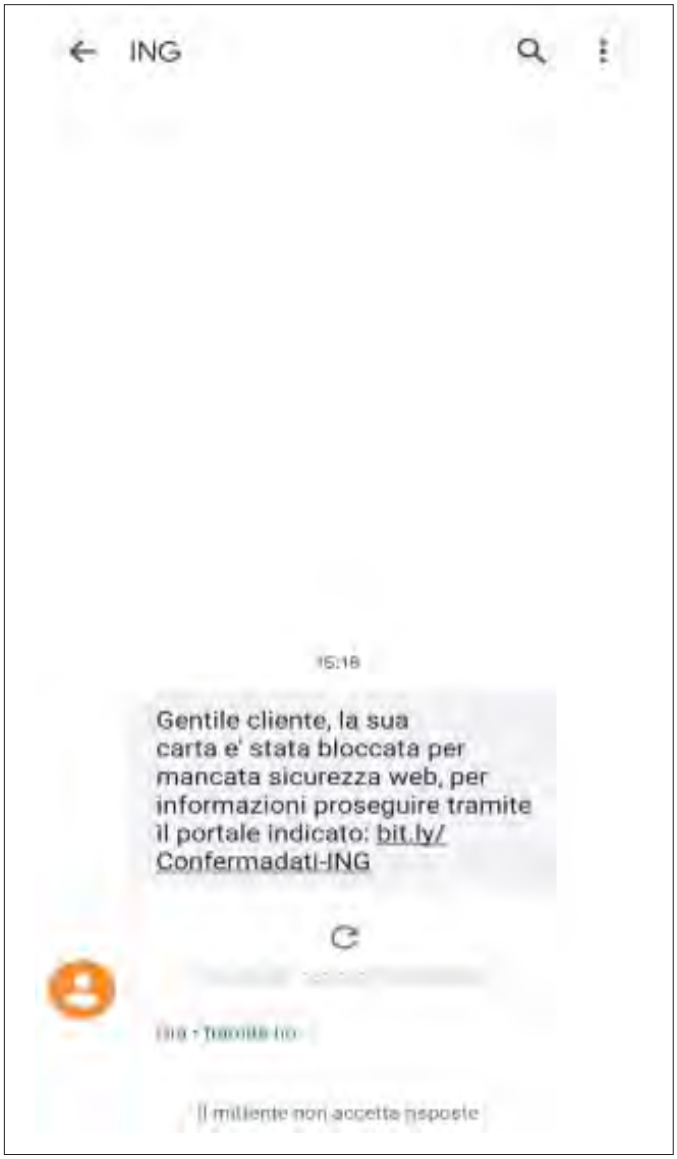
A questo riguardo è stato predisposto il nuovo applicativo informatico "VE.R.DI.", destinato alle attività di analisi del rischio sulle persone fisiche e di ausilio alla determinazione sintetica del reddito.

Si tratta di uno strumento innovativo che sarà oggetto di implementazioni e miglioramenti volti ad ottimizzarne le funzionalità.

→ Enfasi sull'azione che provoca l'infezione, ovvero il pulsante «clicca qui»

→ Nel primo caso si sfrutta l'inevitabile curiosità di scoprire di che pacco si tratti

→ Nel secondo caso: il blocco di una carta è spesso un'eventualità che genera allarme ed apprensione
→ L'attaccante sfrutta questi sentimenti per spingere la vittima a fornire i dati richiesti

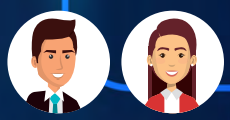


Nel frattempo, in azienda...

Martina

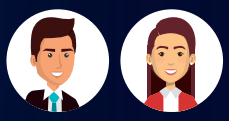
Matteo

No Name



Matteo riceve una mail dalla collega Martina con la quale ha frequenti scambi di posta. L'e-mail di Martina è infatti una risposta ad un messaggio di diverse settimane prima e invita Matteo a prendere visione di un documento linkato. I toni sono insolitamente secchi ma è già capitato che Martina abbia avuto una giornataccia. Matteo clicca sul link al documento e gli vengono richieste le credenziali. Matteo non si pone alcun problema: è un'e-mail interna, di persona conosciuta, in un contesto attendibile. Inserisce le credenziali.

Pochi istanti dopo dal sito abilmente contraffatto, un programmino automatico riceve i dati e testa automaticamente le credenziali di Matteo su un centinaio di diversi siti tra cui tutti i social network, tutti i drive in cloud esistenti compresi quelli dove Matteo ha le foto dello smartphone, Amazon, Netflix, PayPal... tutto. Laddove le credenziali risultino funzionanti, e mancassero sistemi di autenticazione a più fattori, le password saranno cambiate, i dati esfiltrati alla ricerca di materiale interessante come numeri di carte di credito, account bancari, portafogli di criptomoneta e molto altro. Nel frattempo il criminale informatico festeggia: grazie alle credenziali di Matteo è già dentro la VPN aziendale e sta frugando alla ricerca di altri dati e di vulnerabilità utili per preparare il «colpo grosso».



Matteo è perplesso. Chiama Martina che però non risponde, è in call. Ne parla con il suo collega di ufficio che ha ricevuto la stessa e-mail ma l'ha ignorata in quanto era evidentemente phishing. Matteo si sente in imbarazzo e decide di non dire niente a nessuno. Dopotutto l'allegato non si è mai aperto, era una pagina bianca, e le credenziali inserite non hanno funzionato. In ufficio poi ci sono potenti antivirus. Decide che no, non ha voglia di farsi sgridare da quelli dell'IT, cancella l'e-mail, svuota il cestino, per sicurezza. «Non è successo niente».

PHISING: I CONSIGLI DEGLI ESPERTI

→ Diffidare, prendere tempo, dubitare.
Quando una e-mail invita a seguire un link o a inserire dati è meglio fermarsi un attimo a pensare;

→ Attenzione agli indirizzi contraffatti «quasi uguali» agli originali. Non fermarsi al nome «in chiaro» del mittente, ma verificare il reale indirizzo (i vari client di posta elettronica offrono sempre questa possibilità). Anche gli URL (indirizzi di Siti Internet) vengono spesso falsificati con una metrica ingannevole (es. postepay.xzykjh.eu);

→ Se una situazione sembra anomala, probabilmente lo è. Fare una telefonata all'help desk o alle parti in causa. Verificare. Nessuna brutta figura, si tratta solo di dimostrare attenzione;

→ Attenzione al «Principio di Autorità».
Le multe stradali e le sanzioni dell'Agenzia delle Entrate non arrivano via e-mail. Ragionare con freddezza. Alle banche non occorrono credenziali o PIN dispositivi. Ricordare che nessuno regala niente, tantomeno via e-mail o via Whatsapp;

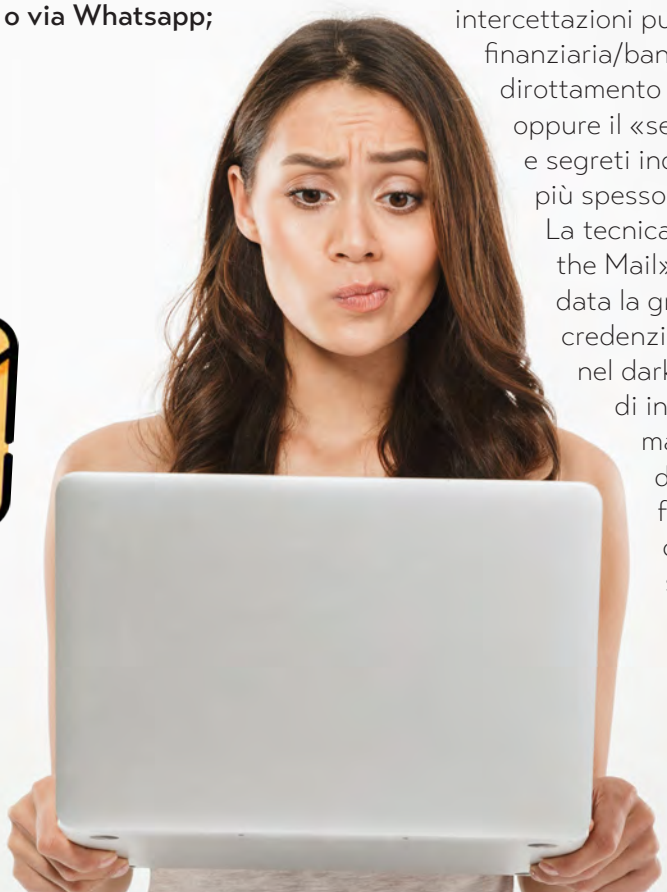
→ Attenzione agli allegati!
Se richiedono ulteriori azioni dopo l'apertura, come l'attivazione di macro o inserimento di credenziali diffidare e contattare un esperto;

→ Attenzione al linguaggio.
La maggior parte delle e-mail di phishing presenta qualche anomalia sintattica o linguistica nel testo. Può essere una sfumatura o un errore grossolano derivato dalla scarsa conoscenza dell'italiano da parte dell'autore o da traduzioni automatiche;

→ Anche la formattazione delle e-mail di phishing tende spesso ad enfatizzare l'azione che l'attaccante vuole che venga compiuta, come ad esempio «Clicca QUI per ottenere il rimborso».

LE INTROMISSIONI

Tramite una tecnica di compromissione di sistemi denominata «Man in the Middle» i criminali si inseriscono a vario livello in un canale di comunicazione tra due parti, spesso cliente e fornitore. L'effetto combinato di queste intercettazioni può essere una frode finanziaria/bancaria giocata sul dirottamento di fondi/pagamenti oppure il «semplice» furto di dati e segreti industriali o, sempre più spesso, entrambe le cose. La tecnica di attacco «Man in the Mail» è molto comune, data la grande disponibilità di credenziali valide in vendita nel dark web. Un'altra tecnica di intercettazione può manifestarsi a livello della navigazione, falsificando i server DNS, che dirottano il traffico su siti perfettamente contraffatti, nati per sottrarre credenziali, carte di credito o documenti personali.



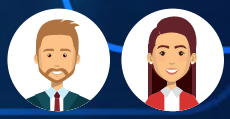
VLADYM DROBOT/FREEPIK.COM

Nel frattempo, in azienda...

Martina

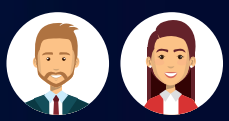
John

No Name



John lavora da anni presso gli uffici amministrativi di una importante azienda di trading olandese. L'importazione di macchinari dall'Italia è il loro core business. Questa mattina John ha ricevuto da Martina, responsabile amministrativo di una azienda del Varesotto con cui lavora da anni, una insolita richiesta. Martina sollecita il pagamento di una grossa fattura in scadenza indicando le coordinate di un conto corrente inglese, invece del solito conto italiano. Mentre prepara il bonifico pensa che, probabilmente, la Brexit ha modificato gli scenari finanziari ed economici.

Dopo settimane di intercettazioni della posta tra John e Martina, l'intruso è emozionato. Il malware che ha installato nel PC di Martina sta iniziando a dare i suoi frutti e finalmente ha potuto mettere le mani su una fattura estero molto sostanziosa. Creare un falso sollecito in PDF per John indicando per il pagamento l'IBAN del conto inglese, che ha aperto online poche ore prima, usando documenti altrui comprati online, è stato un gioco da ragazzi. Il vantaggio di operare sull'estero è che si usa l'inglese e non occorre scervellarsi a tradurre dall'italiano. Una notifica dal suo cellulare con SIM intestata ad un prestanome gli conferma che il bonifico è arrivato. Con pochi colpi di mouse trasferisce l'intera cifra sul suo portafoglio di BitCoin e poco dopo fa sparire tutte le sue tracce. Anche se è sicuro che per poche decine di migliaia di euro nessuna autorità pubblica si prenderà il disturbo di indagare.



Martina inoltra distrattamente al capo l'e-mail di John che assicura di aver pagato quanto in scadenza. Prossimamente avrà la disponibilità della grossa cifra nel conto. Si tratta solo di aspettare qualche giorno e poi potrà pagare a sua volta alcune grosse fatture in scadenza. «Per fortuna che gli olandesi pagano sempre puntuali, quasi in anticipo», pensa.

L'INTERDIZIONE DEI SERVIZI

Gli attacchi «denial-of-service» (Dos o DDos) consistono nell'inviare enormi flussi di traffico a sistemi, reti, siti Internet, per esaurirne le capacità di risposta in tempi accettabili. Le risorse vengono insomma saturate. Ciò comporta il classico stallo del servizio e il suo conseguente mancato utilizzo legittimo. Questo tipo di attacchi è più frequente nell'ambito dell'attivismo digitale, ma ultimamente è entrato a far parte del set di strumenti utilizzato dai gruppi di criminali per ricattare aziende ed istituzioni.
Non è possibile fermare un DDos attack senza la piena collaborazione dei gestori delle reti pubbliche, gli unici in grado di identificare la provenienza del traffico malevolo e in qualche modo filtrarlo prima che saturi le linee della vittima. Per questo motivo, le contromisure contro tale eventualità dovrebbero far parte delle policy di sicurezza di chi è esposto a tale rischio.

FREEPIK.COM

Nel frattempo, in azienda...

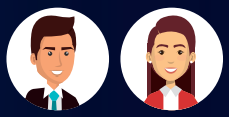
L'attacco cryptolocker della settimana precedente aveva messo in ginocchio l'azienda. Tutto fermo tranne le e-mail. Non si riusciva a spedire, a fatturare, a lavorare sui progetti. Anche in produzione un paio di Centri di Lavoro erano fermi. Insomma, un disastro. I ragazzi dell'IT hanno però fatto miracoli e quel venerdì mattina la situazione sembra essere decisamente migliorata, senza peraltro pagare un centesimo ai ricattatori. Martina, in smart working forzato, accende il suo portatile e si collega alla VPN aziendale per cercare di recuperare un po' del mostruoso arretrato che si è accumulato con questo incidente. La rete è lentissima, non va. Prova ad accedere dalla intranet aziendale, ma è totalmente fuori servizio, così come il sito aziendale. Chiama in azienda, ma il nuovo sistema telefonico non dà segni di vita. Al cellulare personale l'IT Manager le riferisce che sono sotto attacco e che al momento non può fare altro che aspettare.

L'organizzazione di criminali informatici che ha preso di mira l'azienda di Martina non ha affatto gradito che non vi sia mai stato nessun tentativo di contatto con loro, nemmeno per negoziare un riscatto. Ne va della credibilità del gruppo. L'azienda deve essere messa in condizioni di non poter operare. Viene quindi scatenato un DDoS attack su larga scala. Le reti di comunicazione esterne, il sito e tutti i servizi esposti aziendali vengono presi di mira da una vera e propria inondazione di pacchetti internet, provenienti da dispositivi compromessi sparsi per il mondo e nella disponibilità dell'attaccante. Una situazione in grado di mettere di nuovo in ginocchio l'azienda.

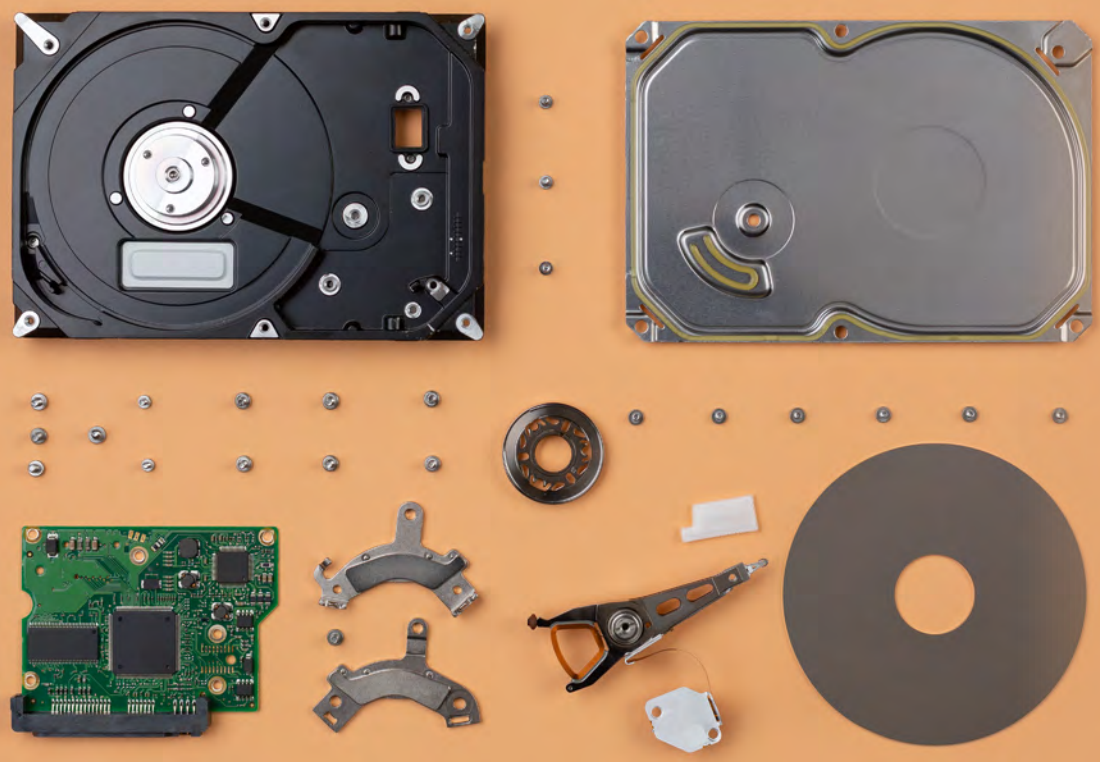
Martina

Matteo

No Name



Matteo chiama il reparto IT per chiedere quando pensano di poter risolvere il problema. Dopo giorni di inattività forzata quell'ulteriore blocco non ci voleva proprio. Il reparto IT risponde di avere le mani legate e che dovranno intervenire per forza il carrier di telecomunicazioni ed i vari service provider per bloccare il traffico ostile a monte. «A proposito, Matteo» chiede il Responsabile, «sai che la prima intrusione, quella che ha scatenato tutto è avvenuta utilizzando le tue credenziali? Per il momento le abbiamo disabilitate. Dobbiamo parlare».



SERGIO ROJO/FREEPIK.COM

ATTACCO ALLE VULNERABILITÀ

Si tratta di attacchi che prendono di mira il perimetro esterno delle reti aziendali, cercando di violarne la sicurezza iniettando sequenze in grado di sfruttare vulnerabilità note nei sistemi, oppure tentando di utilizzare delle credenziali attingendo a database in vendita nel dark web o vocabolari di miliardi di combinazioni precalcolate (attacchi a forza bruta). Generalmente queste attività sono portate avanti da applicazioni automatiche sguinzagliate sulla rete. In alcuni casi se ne occupa personalmente un essere umano, dopo una fase di analisi e studio che può essere individuata e fermata per tempo con gli opportuni strumenti di prevenzione. Se le vulnerabilità non sono note fino al momento dell'attacco, lo stesso prende il nome di Zero-Day. Quest'ultima eventualità è spesso la più catastrofica perché può portare alla compromissione contemporanea di milioni di sistemi in tutto il mondo, creando una seria minaccia alla continuità di una molteplicità di servizi comuni tra cui l'energia, la sanità, l'ordine pubblico ecc.
Questo è uno dei motivi per cui la sicurezza deve essere messa a tema prima di affrontare un qualsiasi progetto informatico. Mettere la sicurezza tra i requisiti di partenza aiuta il lavoro di chi poi dovrà proteggere l'infrastruttura.

PERDITA DI DATI

La perdita o la diffusione di dati può essere una conseguenza, spesso la più grave, di una delle altre principali minacce, oppure può essere un evento a sé stante derivante da errori umani, imperizia, o eventi esterni come incidenti, furto di dispositivi o altro che possono avvenire in tutto il ciclo di vita del dato. Spesso anche quando il dato giace ormai dimenticato su qualche supporto dismesso, come vecchi PC in disuso, chiavette USB, cellulari.
Si parla quindi di perdita (data loss) quando le informazioni critiche (o in qualche modo utili) vengono definitivamente perse o rese inaccessibili. Si parla invece di diffusione o fuga (data leak) quando si verifica l'accesso di terzi non autorizzati ai dati anche se l'azienda continua ad averne la disponibilità. Ad esempio, quando viene effettuata una copia non autorizzata. Contro queste due eventualità si concentrano diverse strategie di prevenzione che operano sulla protezione e il monitoraggio degli accessi.

È bene precisare che i cosiddetti «Data Breach», cioè la diffusione o compromissione di dati personali da parte di soggetti non autorizzati, possono essere conseguenze di una violazione della rete, ma spesso

(continua a pag. 28)

Nel frattempo, in azienda...

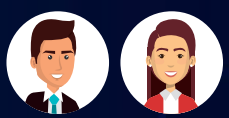
Martina

Matteo

No Name

Matteo in smart working ha sempre lavorato molto bene, gestendosi il tempo e riuscendo finalmente a conciliare la sua passione per il crossfit con l'impegnativa attività professionale da giovane manager in piena ascesa. Un solo problema però lo assilla da tempo: non riuscire ad accedere ai progetti per discutere con i clienti davanti al disegno come fa in ufficio, cliccando un'icona con scritto RDP «qualcosa». Durante un'assenza forzata per un infortunio «di palestra» però, Matteo grazie all'intercessione del suo capo, riesce finalmente a poter accedere a quel benedetto CAD anche da casa. Sembra un sogno.
«Ok ma per un tempo limitato» dice l'IT, «massimo una giornata o due e ricordati di uscire dall'account quando hai finito».

Lo scanner, un programma spia, sguinzagliato sulla rete aziendale da un attaccante incaricato da un'azienda concorrente straniera, dà finalmente il sospirato esito positivo. C'è una falla. Si può entrare. Da quello spiraglio di accesso lasciato esposto su Internet, con alcuni semplici passaggi e grazie ad alcune vulnerabilità note, è possibile prendere il controllo della macchina esposta. L'attaccante inizia ad esplorare la rete aziendale organizzando la sottrazione sistematica e silente di tutti i progetti e dei riferimenti di tutti i clienti. «Un giorno da qualche fiera in qualche paese in via di sviluppo arriverà una foto di un macchinario identico al loro tranne che per il marchio, allora forse si faranno qualche domanda» sogghigna l'attaccante.



Matteo realizza di non essersi «sloggato» nella precedente sessione che trova ancora come l'ha lasciata la sera precedente. Del resto, era in ritardo e doveva raggiungere il box di crossfit entro pochi minuti per le gare. «Per una volta cosa vuoi che succeda?».

anche di errori umani nella configurazione della stessa. L'approccio tradizionale nella protezione delle reti è sempre stato quello di proteggere i dati da accessi esterni senza preoccuparsi troppo di quello che accade dall'interno. Pianificare gli interventi separando i due concetti, quello della sicurezza della rete e quello della sicurezza dei dati, è diventato ormai indispensabile.
Per realizzare questa separazione vengono in aiuto gli strumenti autorizzativi e crittografici che possono limitare fortemente il rischio di accessi non autorizzati anche se la rete è stata violata. Adottando strati di protezione adeguati, un attacco alla rete porterebbe infatti all'accesso di informazioni totalmente illeggibili ed indecifrabili.
Anche le procedure sanzionatorie del GDPR e gli obblighi di notifica al Garante dei Data Breach, non riguardano la mera violazione di rete, ma fanno riferimento esclusivamente alle sue conseguenze reali in termini di diffusione, distruzione o alterazione di dati personali. Paradossalmente alcuni incidenti informatici molto gravi che non hanno comportato però impatti in questo senso, non prevedono l'obbligo di notifica.

LINK E RIFERIMENTI

Dal sito del Garante:
→ definizione di Data Breach e cosa fare nel caso in cui si verifichi
www.garanteprivacy.it/regolamentoue/databreach

→ principi generali del trattamento di dati personali
www.garanteprivacy.it/home/doveri

IL FURTO DI IDENTITÀ

Una delle conseguenze più gravi dei Data Breach è rappresentata dal furto di identità o impersonificazione. Dati e documenti, organizzati in comode tabelle, vengono venduti in aste clandestine nel Dark Web. Chi li acquista potrà facilmente predisporre degli attacchi mirati e credibili con la stessa semplicità con la quale in ufficio facciamo un "mail merge".
Ad esempio, di recente, una importante casa automobilistica ha subìto il furto dei dati di milioni di clienti, con informazioni dettagliate riguardo il modello di auto acquistata, gli allestimenti, il tipo di pagamento, l'e-mail, il telefono, ecc. Possiamo immaginare nel prossimo futuro una intensa attività volta a trarre in inganno questi clienti con comunicazioni di vario genere, come ad esempio falsi richiami.
Corrispondenze tutte apparentemente provenienti dalla casa automobilistica e rese più credibili da dettagli esatti sul modello di auto in loro possesso.
In ambito Social Network questo tipo di violazione può avere conseguenze molto gravi in quanto l'attaccante può entrare in possesso di informazioni personali di tutta la nostra rete di contatti, comprese foto personali e familiari.

Nel frattempo, in azienda...

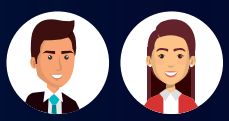
Martina

Matteo

No Name

Matteo ha sempre pensato che il segreto del suo successo fosse di non concedere nemmeno un centimetro del suo vantaggio competitivo alla concorrenza, soprattutto quella interna. «Ce l'ho sui miei file di Excel, non scappa niente» è solito dire al suo capo, che periodicamente riceve degli splendidi report e non si pone nessun problema. Del resto, il sistema ERP aziendale è talmente noioso e farraginoso da far scappare la voglia a chiunque di usarlo. Il Laptop aziendale poi, non ne parliamo. Lento e con strani meccanismi che puzzano di «controllo». Meglio usare il suo nuovissimo Core i7 di ultima generazione.

Quando Matteo si trova davanti al carabiniere per sporgere denuncia non riesce quasi a parlare. «È stato un attimo» continua a ripetere. «Stavo andando al parchimetro e mi hanno rubato giacca, borsa, portatile e cellulare».



Il giorno dopo spiega al suo capo che no, non c'è un backup, era il suo pc personale, del resto. Non c'era una crittografia e nemmeno una password. Una serie di informazioni commerciali vitali per l'azienda erano andate perse nella migliore delle ipotesi, oppure erano cadute in mani sbagliate. Il cellulare aziendale era spento in borsa. Tutti i contatti e la posta erano stati spostati sul suo nuovissimo iPhone personale, molto più veloce. No, il blocco del telefono no, perché il Face ID con la mascherina è un disastro e lo aveva disabilitato...

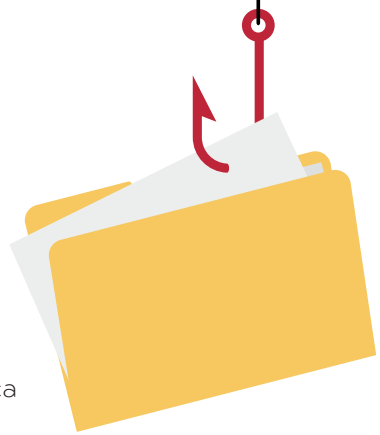
PERCHÉ RISCHIO? COSA RISCHIO?

Volendo semplificare molto, possiamo individuare due grandi tipologie di rischio per le nostre imprese: il rischio casuale e l'attacco mirato.

RISCHIO CASUALE

Nel primo caso, l'attaccante, spesso privo di competenze tecniche particolari, acquista per pochi dollari nel dark web servizi on-demand preconfigurati, per lanciare un attacco alla cieca su larga scala nel web. È il caso del phishing generico, di attacchi alle vulnerabilità attuati da software di scansione (Bot), dello SPAM generico. Qualcosa di simile alla pesca a strascico, che porta sempre qualche risultato confidando sui grandi numeri e sulle probabilità di successo.

ATTACCO MIRATO



Nel secondo caso, ben più pericoloso, l'attaccante o una organizzazione di criminali (ultima tendenza) prende di mira proprio la nostra azienda e prepara e pianifica l'attacco meticolosamente. Nelle situazioni più complesse saranno esfiltrati dati, progetti, documenti e dati bancari. Sarà valutata l'escalation che l'attacco dovrà avere. Se l'intrusione ha finalità economiche verranno valutate le tecniche di backup e rese inefficaci. Verrà valutata la potenza economica dell'azienda per richiedere, al momento opportuno, un riscatto adeguato sotto il triplice ricatto di diffusione dei dati, perdita definitiva degli stessi e in ultimo di attacchi denial-of-service verso i servizi esterni (sito, connessione a Internet, ecc...).

Di contro, se l'intrusione ha finalità di spionaggio industriale, gli attaccanti faranno perdere le proprie tracce terminando il loro lavoro in modo silenzioso. Sempre più spesso, infine, si riscontrano attacchi mirati a personalità di rilievo nell'azienda facendo leva sulla loro autorevolezza e capacità di spesa, creando situazioni di impersonificazione volte a mettere in soggezione un subordinato (spesso amministrativo) e spingerlo ad effettuare pagamenti in una situazione di apparente emergenza.

IL DECALOGO

RAWPIXEL.COM-BENJAMAS/FREEPIK.COM

Una volta conosciute le più diffuse minacce e inquadrata la tipologia di rischio a cui è soggetta l'impresa, nasce inevitabilmente l'urgenza di fare concretamente qualcosa di più per proteggere adeguatamente gli asset aziendali e quindi, in ultima analisi, cercare di garantire la continuità dell'attività, prevenendo incidenti di ogni genere.
Come spesso accade si può procedere in ordine sparso, facendosi guidare dalla «minaccia del momento», oppure tentare di approcciare una strategia seguendo un metodo.
Confindustria Varese propone qui di seguito un piccolo decalogo organizzato per schede.
Questi dieci suggerimenti sono stati selezionati cercando di coprire tutti i temi che concorrono alla Sicurezza di dati e sistemi in una tipica Piccola e Media impresa, ben consapevoli tuttavia della sfida della complessità che ogni giorno le aziende si trovano a fronteggiare e delle peculiarità di ciascuna.
Come approcciare al Decalogo? Il suggerimento è di seguire questo metodo operativo:

- → **Definire come si posiziona la propria impresa rispetto a quel punto del decalogo;**
- → **Analizzare i rischi che la propria impresa sta correndo rispetto a quel punto;**
- → **Definire, attuare un realistico obiettivo di miglioramento su quel punto;**
- → **Definire ed attuare controlli e revisioni periodiche.**

Sul concetto di miglioramento, occorre precisare che anche la mitigazione di una criticità rappresenta appunto un miglioramento, essendo ormai chiaro a tutti che il "rischio zero" non esiste.

1 MAPPARE ATTORI, RUOLI E RESPONSABILITÀ

2 FORMAZIONE E INFORMAZIONE

3 GDPR POLICY E CERTIFICAZIONI

4 PRIVILEGI MINIMI

5 PROTEZIONE DELLA POSTA E DEL PERIMETRO

6 BACKUP E CLOUD

7 AGGIORNAMENTI

8 DISPOSITIVI MOBILI

9 MONITORAGGIO, PIANO GESTIONE INCIDENTE E DISASTER RECOVERY

10 ASSICURAZIONI

1

MAPPARE ATTORI, RUOLI E RESPONSABILITÀ

È opportuno iniziare questo percorso incaricando una persona in azienda che faccia da punto di riferimento per tutte le attività legate alla sicurezza informatica. Il profilo ideale ha un ruolo di responsabilità, ha visibilità su tutti i processi chiave ed è in grado di relazionarsi adeguatamente con le diverse figure aziendali. Le competenze tecniche sono utili, ma non indispensabili. Naturalmente il dialogo costante e proficuo con l'IT aziendale (se presente) o con i fornitori di tecnologia, rappresenta un elemento imprescindibile.
È assolutamente indispensabile mappare tutti gli elementi distinti che concorrono a creare il nostro Sistema Informativo Aziendale. **La tabella della pagina seguente può essere fonte di ispirazione.**

Per completare la visione d'insieme, può essere molto utile recuperare e revisionare il lavoro fatto in occasione dell'entrata in vigore del GDPR.

COSA FARE?

→ **Cercare di ottenere una visione di insieme il più possibile corretta e non trascurare quello che succede all'esterno dello stretto perimetro aziendale, nei dispositivi utilizzati per lo Smart Working, siano essi aziendali o personali.**

→ **Individuare consulenti, fornitori, tecnici che hanno accesso a dati aziendali (non solo quelli personali ma anche quelli critici per il business come i progetti).**

→ **È importante rilevare i cosiddetti «shadow-IT» ovvero tutte quelle soluzioni implementate e usate in azienda senza autorizzazione, e che quindi sfuggono ad ogni controllo o policy di sicurezza.**

MAPPATURA RISORSE E ACCESSI
ESEMPIO DI COMPILAZIONE

ELEMENTO DEL SISTEMA	CHI VI ACCEDE (QUANTI)	PERCHÉ VI ACCEDE	COME VI ACCEDE
RETE DI PC / FILE SU SERVER O CLOUD	IMPIEGATI AMMINISTRATIVI, MARKETING, DIREZIONE 70 PERSONE	CORRISPONDENZA, LETTERE COMMERCIALI, PREVENTIVI	PERSONAL COMPUTER
FILE DI PROGETTO / CAD	PROGETTISTI, MONTATORI MANUTENTORI 13 PERSONE	PROGETTAZIONE E ASSISTENZA TECNICA	PC / MAC WORKSTATION
SISTEMA GESTIONALE RP	AMMINISTRATIVI MAGAZZINO 90 PERSONE	CONTABILITÀ SPEDIZIONI	TERMINALE
FIREWALL, ROUTER, VPN, WIFI	IT MANAGER / FORNITORE 3 PERSONE	CONFIGURAZIONI E MANUTENZIONE	PERSONAL COMPUTER (PROTOCOLLI SICURI)
POSTA ELETTRONICA	TUTTI 220 PERSONE	ATTIVITÀ	PC / MAC APPARATI MOBILI
RETE DI FABBRICA / MACCHINE	IT MANAGER, SISTEMISTA, VENDOR, CENTRI DI LAVORO 16 PERSONE	CONFIGURAZIONE, ACCESSO DATI FABBRICA, TELEASSISTENZA	VPN, SIM DATI A BORDO MACCHINA

DA DOVE VI ACCEDE	REFERENTE INTERNO	FORNITORI COINVOLTI	POLITICA DI BACKUP
UFFICIO O DA REMOTO	IT MANAGER, SISTEMISTA	ABC SRL, CDE SPA	GIORNALIERO SOLO SERVER E STORAGE SU NAS LOCALI RETENTION 10 GIORNI
UFFICIO O DA REMOTO	IT MANAGER/ CAPO UFFICIO TECNICO	AUTODESK	GIORNALIERO RETENTION 20 GG + ARCHIVIAZIONE MENSILE
UFFICIO	IT MANAGER, RESPONSABILE AMMINISTRAZIONE	CDE SPA	NOTTURNO E PAUSA PRANZO RETENTION 30 GG + ARCHIVIAZIONE ANNUALE
UFFICIO O DA REMOTO	IT MANAGER, SISTEMISTA	CONSULENTE X	(COPIE FILE CONFIGURAZIONE)
UFFICIO, DA REMOTO O MOBILE	IT MANAGER	CDE SPA	NESSUNO
SOLO FABBRICA O TELEASISTENZA	IT MANAGER, RESPONSABILE PRODUZIONE	ACG SRL...	NESSUNO

2

FORMAZIONE E INFORMAZIONE

Il «Fattore Umano» rappresenta il primo e più grave rischio per la Sicurezza.
Le misure tecnologiche da sole non bastano. Occorre mantenere alta l'attenzione di tutti i collaboratori sulle molteplici tipologie di rischio che si incontrano nell'attività lavorativa e nella vita privata. Una volta definita la classe di rischio delle varie aree aziendali, la strada della formazione periodica e dell'informazione puntuale su rischi emergenti è sempre vincente, perché motiva i collaboratori e crea competenza, consapevolezza e collaborazione.

COSA FARE?

→ **Fare formazione allenando i colleghi a riconoscere le situazioni «sospette» e rinnovarla almeno ogni sei mesi. In caso di nuove minacce emergenti, fare «informazione» mediante comunicazioni «al bisogno», ricche di esempi e contestualizzate a casi reali;**

→ **Prevedere la formazione periodica per il trattamento sicuro dati personali (GDPR). La stessa è, infatti, obbligatoria ai sensi del GDPR;**

→ **Valutare una sensibilizzazione personalizzata per le aree più a rischio come, ad esempio, gli amministrativi o, in generale, chi ha potere di disporre pagamenti e quindi essere vittima di truffe;**

→ **Accompagnare alla formazione per gli amministrativi la stesura di procedure di sicurezza per la verifica incrociata di pagamenti su estero per la prevenzione di truffe. Condividere le procedure con i clienti esteri;**

→ **Sensibilizzare i vertici dell'azienda ai rischi specifici. Accompagnare la formazione commissionando un'indagine mirata sulla situazione aziendale (domain Threat Intelligence) ad una azienda specializzata affidabile e seria in grado di operare restando nell'alveo della legalità.**

3

GDPR POLICY E CERTIFICAZIONI

Il Regolamento Europeo sulla Protezione dei Dati (GDPR) è stato spesso vissuto dalle imprese come l'ennesima incombenza burocratica. Il percorso di conformità al GDPR può, al contrario, rappresentare un'occasione da non perdere per mappare in modo sistematico i trattamenti di dati personali che avvengono in azienda e attuare misure organizzative e tecnologiche di protezione e mitigazione dei rischi.
L'altro importante monito che arriva dal GDPR è quello di pensare alla protezione dei dati by design, ovvero quando si sta ancora progettando un prodotto o un servizio e non chiudere le falle quando ormai gli errori sono stati commessi.
Oltre al regolamento europeo, la cui applicazione è obbligatoria negli stati membri, esistono diversi framework di sicurezza e strumenti di certificazione come la ISO 27001 che possono essere utilizzati per certificare a clienti e fornitori l'utilizzo di strumenti di gestione e controllo della Sicurezza delle Informazioni. GDPR e ISO 27001, così come altri framework, possono operare in sinergia per assicurare la riservatezza, l'integrità e la disponibilità dei dati e servizi critici in azienda.

COSA FARE?

→ **Revisionare tutto il lavoro fatto per il GDPR almeno annualmente, aggiornando il documento di conformità, definendo degli obiettivi di miglioramento e dandogli attuazione;**

→ **Valutare la creazione di una policy aziendale (regolamento) per l'utilizzo di sistemi e il trattamento dei dati, accompagnato da un percorso di formazione specifico: rappresenta uno strumento ideale per condividere regole e procedure con uno strumento snello ed efficace;**

→ **Se l'azienda riceve continue richieste di assessment sulla sicurezza da parte di clienti, fornitori o altri soggetti, forse è venuto il momento di affrontare un percorso di certificazione a valenza internazionale come le ISO 27001.**

FREEPIK.COM

4

PRIVILEGI MINIMI

Nel punto 1 abbiamo creato una mappa di tutti gli elementi che compongono il Sistema Informativo. Con questa informazione possiamo attivare una procedura attraverso la quale verificheremo ad ogni assunzione (e periodicamente per tutto il personale) l'adeguatezza dei privilegi di accesso a dati e sistemi. Per ogni elemento del sistema adottiamo la strategia dei «Privilegi Minimi»: ogni figura aziendale deve avere accesso solo alle informazioni che gli sono necessarie e per il tempo necessario. Vale l'esempio del «mazzo di chiavi». A ciascuno vengono assegnate solo quelle indispensabili per accedere agli ambienti autorizzati. Se eccezionalmente ne occorre una in più per uso sporadico, al cessare dell'esigenza, essa viene prontamente restituita.

Sempre in tema di esempi, se consegniamo il nostro cellulare a qualcuno, con l'intenzione di mostrargli un'unica immagine e costui inizia a sfogliare la gallery liberamente, stiamo sperimentando gli effetti di una violazione (lettura non autorizzata) a fronte di un privilegio eccessivo (il cellulare dato in mano). Se avessimo mostrato la foto tenendo lo smartphone saldamente nelle nostre mani (criterio di protezione) questa lettura non autorizzata non sarebbe avvenuta.
In ambito aziendale la strategia dei privilegi minimi si realizza con un'attenta profilazione e revisione periodica degli utenti, dei dati condivisi e dell'accesso alle applicazioni.
È indispensabile applicare una policy per la gestione delle credenziali che saranno sempre individuali, con password complesse rinnovate di frequente. Il furto di credenziali valide rappresenta l'emergenza più grave nel mondo della Sicurezza Informatica e il personale deve essere sensibilizzato ed allenato a non «cadere in trappola».
Questo insieme di accorgimenti aiuterà l'impresa a rispettare le normative sulla Privacy, a ridurre i rischi di perdita o compromissione di dati in caso di incidente.

COSA FARE?

→ **Mantenere alta l'attenzione sulla riservatezza e adeguatezza delle credenziali senza eccezioni e senza deroghe. Revisionare periodicamente la situazione, chiudendo accessi temporaneamente concessi;**

→ **Fare attivare, laddove possibile, adeguati sistemi di autenticazione a più fattori (MFA) e fare in modo che la protezione sia proporzionale al rischio;**

→ **Non considerare gli SMS, quando utilizzati come elemento di validazione secondaria, come sicuri ed affidabili in senso assoluto. Il «furto» del numero di telefono è possibile, con documenti ottenuti in modo fraudolento;**

→ **I sistemi di Crittografia oggi sono in grado di garantire un'eccellente protezione dei dati riservati da letture non autorizzate anche in caso di esfiltrazione o incidenti involontari. Spesso la protezione crittografica è attivabile con pochi click su diversi dispositivi. Nel caso invece di dati condivisi critici, è bene rivolgersi a servizi professionali di consulenza;**

→ **Valutare l'introduzione di un sistema di gestione unificata dell'identità degli utenti (Identity Management). Renderà meno complesso questo processo fondamentale;**

→ **È indispensabile separare le reti dati laddove necessario, come ad esempio la rete di fabbrica da quella degli uffici segregando l'hardware a bordo macchina, spesso obsoleto e non aggiornabile, dal resto della rete.**

5

PROTEZIONE DELLA POSTA E DEL PERIMETRO

La maggior parte delle minacce alla sicurezza di dati e sistemi, in qualsiasi azienda, passa dalla posta elettronica (circa il 90%). Altre volte, anche se più raramente, direttamente dalla connessione ad Internet, in assenza di adeguate protezioni.
L'introduzione improvvisa e poco pianificata dello smart working ha allargato alle case di tutto il personale il perimetro di sicurezza dell'azienda, ed ora espone l'impresa a nuovi rischi mai ponderati prima. Policy, protezione avanzata della posta, delle reti e dispositivi aziendali (anche mobili) e dei punti di accesso, sono aspetti irrinunciabili per la sicurezza di dati, e per la continuità del business.
Attenzione: la sicurezza informatica non si ottiene con la mera somma di tecnologie di protezione. Occorre prestare la massima attenzione al «Fattore Umano», curando sempre primariamente la formazione e l'informazione sui pericoli emergenti.
È fondamentale non trascurare poi la sicurezza fisica degli ambienti, spesso cruciale per la disponibilità e l'integrità dei dati. I server e le apparecchiature critiche devono essere ricoverati in ambienti consoni e protetti e non in magazzini, sottoscala, ripostigli. Evitare rischio polvere, calore, allagamento, cali di tensione. Meglio piuttosto valutare l'ipotesi di spostare in Cloud dati e sistemi, specie quelli indispensabili all'attività aziendale.

COSA FARE?

→ Il primo intervento da effettuare è sempre sul «Fattore Umano». Informare, formare il personale sui rischi e sui comportamenti corretti è l'arma più efficace in assoluto per la protezione dei dati e degli asset aziendali;

→ Verificare con regolarità l'efficacia dei firewall, antivirus, antispam. È necessario estendere le verifiche anche all'ambito dello Smart Working e ai dispositivi mobili. È fondamentale intervenire subito su eventuali vulnerabilità riscontrate e procedere a tutte le bonifiche necessarie;

→ Intervenire sulle soluzioni di emergenza adottate per la pandemia, come ad esempio i desktop remoti esposti su Internet o altre soluzioni inadeguate, dettate dalla fretta, che si sono poi consolidate;

→ Verificare la sicurezza delle VPN, adottare l'autenticazione a più fattori e valutare l'opportunità di acquisire un servizio di Cloud Security/Web Security a livello DNS per proteggere anche chi opera da remoto;

→ Diversi fornitori di servizi e tecnologia sono in grado di proporre i cosiddetti Penetration Test in grado di mettere in evidenza la gran parte delle vulnerabilità presenti nel «perimetro» aziendale. Si tratta di test non esaustivi, ma senz'altro utili;

→ Revisionare le reti Wi-Fi rivedendo tutta l'organizzazione della sicurezza, le risorse accessibili, le credenziali. Applicare restrizioni sulla concessione delle password ad ospiti e dipendenti e fare in modo che scadano al termine dell'uso;

→ Se la rete Wi-Fi aziendale serve solo per la navigazione, è bene separarla totalmente da quella degli uffici operativi;

→ Se la complessità aziendale lo richiede, valutare un servizio di Monitoraggio e Risposta (SOC - Security Operations Center - e altri servizi evoluti di nuova generazione in grado di prevenire, individuare, mitigare e circoscrivere eventuali attacchi in corso, attuando interventi automatici).

6

BACKUP E CLOUD

«Non servirà un backup. Servirà un restore». Le nuove minacce alla sicurezza impongono un totale ripensamento delle strategie di archiviazione e di backup. Oltre a rispondere ai bisogni tradizionali di ripristino di archivi, oggi il backup è diventato un tassello essenziale per garantire la continuità del business. I criminali informatici lo sanno e faranno di tutto per renderlo inservibile per spingere a pagare un riscatto per riavere i propri dati. Oggi, con una spesa sostenibile da tutti, è possibile adottare politiche di archiviazione dati e di backup, con il supporto delle tecnologie Cloud, che possono contribuire a ridurre sensibilmente l'impatto sull'integrità e disponibilità dei dati in caso di incidente. È importante però privilegiare sempre un ambiente Cloud serio, affidabile e ridondato, avendo cura di verificare che i dati personali siano archiviati, in osservanza al GDPR, in un Paese dell'Unione Europea e che vengano mantenuti adeguati profili di sicurezza in tutto il ciclo di vita del dato. Occorre anche prestare attenzione alle possibili problematiche geopolitiche ed ingerenze straniere nella gestione dei grandi Cloud.

COSA FARE?

→ **Predisporre policy sui dati condivisi, evitando che gli stessi vengano polverizzati su supporti inadeguati o non autorizzati (chiavette, dischi, cloud privati) a rischio di diffusione o distruzione;**

→ **Procedere ad una revisione ed aggiornamento frequente sull'adeguatezza della politica di backup. Verificare se i dati salvati sarebbero sufficienti a consentire una risposta rapida in caso di incidente;**

→ **Effettuare con regolarità delle verifiche sull'efficacia dei backup. Simulare il ripristino di dati e sistemi con un controllo puntuale della reale consistenza di quanto è stato copiato e ripristinato. Se il sistema di backup prevede verifiche automatiche, attivarle;**

→ **Pianificare l'archiviazione in Cloud del backup con adeguati meccanismi allo stato dell'arte rispetto alle ultime tecniche di attacco;**

→ **Valutare lo spostamento in Cloud di eventuali archivi condivisi, mantenendo sempre sotto controllo i diritti di accesso, facendo in modo che gli stessi vengano ereditati automaticamente dai sistemi aziendali;**

→ **Verificare con i fornitori la politica di backup su servizi in data center esterni (es. Sito Internet). Spesso per tenere bassi i costi non è previsto alcun servizio di backup e di ridondanza geografica con il rischio di perdita totale in caso di incidente.**

7

AGGIORNAMENTI

Buona parte degli attacchi ai sistemi informatici, siano essi mirati o «di massa» sfrutta delle vulnerabilità note e già risolte da tempo dai produttori. Una efficiente politica di aggiornamento di tutti i vari componenti del Sistema Informativo aziendale (compresi gli oggetti interconnessi!) è un tassello fondamentale per la sicurezza. Molto spesso anche alcune componenti hardware necessitano di aggiornamenti periodici, proprio per le falle che vengono via via scoperte. È importante quindi individuare software e sistemi a «fine vita» cioè non più aggiornabili, per metterli in sicurezza in vista di una futura dismissione o sostituzione. In alcuni casi le vulnerabilità utilizzate dai criminali sono le cosiddette «Zero-day», ovvero mai rese note prima. Anche in questo caso essere in grado di aggiornare e bonificare tempestivamente i sistemi è fondamentale, ma richiede una capacità di intervento e reazione pianificata per tempo.

COSA FARE?

→ **Disconnettere o portare fuori dal perimetro aziendale tutto l'hardware interconnesso non necessario, soprattutto quello a basso costo e obsoleto (telecamere, lampade wi-fi, stampanti consumer, smart-tv, assistenti vocali...) perché possono diventare punti di accesso alla rete aziendale e utilizzati da malintenzionati per sferrare attacchi o esfiltrare informazioni. Qualsiasi nuovo dispositivo interconnesso entri in azienda, deve essere oggetto di autorizzazione e valutazione circa l'opportunità di collegarlo effettivamente alle reti aziendali;**

→ **Server e PC utilizzati per applicazioni aziendali particolari devono essere aggiornati con la supervisione dei fornitori. è bene non improvvisarsi sistemisti, soprattutto quando si parla di sistemi critici;**

→ **L'aggiornamento dei dispositivi mobili aziendali non deve mai essere trascurato. Un sistema di MDM (gestione centralizzata dei dispositivi) potrebbe aiutare l'azienda a tenere tutto sotto controllo qualora il numero di dispositivi fosse significativo;**

→ **Se si acquistano servizi in Cloud (ad esempio sito web), verificare che nel contratto vi siano impegni da parte del fornitore ad una adeguata politica di aggiornamento delle piattaforme che realizzano il servizio.**

8

DISPOSITIVI MOBILI

Cosa succederebbe se uno dei dispositivi mobili aziendali (Pc, Tablet o Smartphone) dovesse essere rubato, smarrito o rompersi in modo irreparabile, causando la perdita definitiva di tutti i dati contenuti? È opportuno essere a conoscenza di cosa è archiviato nei dispositivi mobili aziendali e di come i dati critici vengono trattati in mobilità e in lavoro da remoto.
Crittografia, Cloud, autenticazione a più fattori, sistemi di gestione e policy aziendali possono essere molto efficaci per azzerare i rischi di fuga o perdita di dati da dispositivi mobili.

COSA FARE?

→ **Riconoscimento biometrico e/o PIN di blocco devono essere obbligatori per tutti i dispositivi aziendali, senza deroghe;**

→ **Crittografia dei dischi, backup dei dati in Cloud con autenticazione a più fattori possono mettere l'azienda al riparo dai rischi di furto, smarrimento o guasto di portatili e tablet;**

→ **Prendere in considerazione l'implementazione di un sistema MDM (gestione dei dispostivi mobili centralizzata). Consentirà di controllare e gestire la sicurezza di tutti i dispositivi aziendali e di intervenire in caso di emergenza, nel rispetto delle normative sulla privacy;**

→ **La Cloud Security/Web Security si può estendere ai dispositivi utilizzati per il lavoro a distanza. Si può così mantenere sotto protezione i dispositivi ovunque si trovino;**

→ **Applicare una policy che disciplini attentamente il trattamento di dati critici o sensibili su dispositivi mobili. No a file abbandonati su smartphone dismessi e dati a familiari, chiavette USB, HDD (hard disk), removibili o drive Cloud privati.**

9

MONITORAGGIO, PIANO GESTIONE INCIDENTE E DISASTER RECOVERY

La maggior parte degli attacchi informatici distruttivi ha una modalità di esordio ed evoluzione che è stata analizzata in precedenza da esperti del settore, anche se difficile da prevenire senza sistemi evoluti di monitoraggio continuo e il supporto di esperti.
È il caso, ad esempio dei famigerati ransomware, cioè attacchi che rendono inservibile il sistema informativo cifrandone tutto il contenuto per poi estorcere all'azienda un cospicuo riscatto per ottenere (senza certezza alcuna) la chiave di decrittazione.
È bene prepararsi a questa o altre eventualità (come ad esempio un evento naturale) con il supporto di esperti che aiuteranno a formulare un piano di prevenzione e gestione di eventuali incidenti, dal più banale al più grave, per accelerare al massimo il ripristino delle attività vitali per il business e adempiere agli obblighi di legge. Sapere esattamente cosa fare, chi coinvolgere ed agire rapidamente può fare la differenza in un momento di grave crisi.
Per le realtà aziendali più complesse stanno diventando sempre più diffusi i sistemi di monitoraggio e intervento rapido, basati su un mix di intelligenza artificiale e presidio umano.

COSA FARE?

→ Le conseguenze di un incidente che renda indisponibili dati e sistemi devono essere valutate periodicamente e in occasione di ogni implementazione significativa del Sistema Informativo. Disporre di un piano di emergenza può fare risparmiare giorni di blocco delle attività;

→ I piani di emergenza devono essere realizzati in collaborazione con i fornitori che spesso possono mettere a disposizione risorse limitate. In questo caso valutare una possibile «escalation» in sinergia con altri soggetti in grado di fornire professionalità e risorse a sufficienza;

→ Nelle analisi, considerare sempre anche aspetti ambientali e di contesto, come ad esempio, la possibile prolungata mancanza di energia, il blocco persistente della connettività Internet o privata verso altre sedi aziendali e tutti gli altri scenari che possano mettere in discussione la disponibilità di dati e sistemi;

→ Le imprese più strutturate possono prendere in considerazione l'ipotesi di acquistare un servizio di monitoraggio continuo (SOC - Security Operations Center - o di altri servizi in grado di bloccare o contenere entro un perimetro limitato un eventuale incidente informatico);

→ In caso di incidente che abbia comportato l'esfiltrazione o comunque la diffusione di dati personali è obbligatorio avviare una procedura di notifica al Garante della Privacy (Data Breach) entro 72 ore dal momento in cui è stata accertata.

NB. *Tale obbligo non sussiste solo per grandi imprese e per attacchi eclatanti, ma vale per ogni perdita di controllo su dati personali che possa comportare eventi avversi significativi per chi ne è vittima, come ad esempio la compromissione di dati anagrafici, credenziali, documenti personali che potrebbero, ad esempio, venire utilizzati per confezionare Spare Phishing, cioè Phishing altamente personalizzato.*

10

ASSICURAZIONI

L'aspetto assicurativo sta assumendo sempre più importanza nell'ambito della Sicurezza. La stipula di una polizza adeguata può aiutare in due modi:
→ fotografare la situazione aziendale attuale ed evidenziare i punti deboli su cui intervenire grazie ai questionari che verranno proposti;
→ fornire all'impresa le risorse per reagire adeguatamente ad una situazione critica.

Le politiche e i prodotti delle compagnie assicurative sono in rapida evoluzione, così come lo è il crimine informatico. È importante scegliere accuratamente il prodotto adeguato e soprattutto non sottovalutare la fase di valutazione del rischio che può essere un'ulteriore opportunità di focalizzare il proprio posizionamento.

COSA FARE?

→ **Non sottovalutare i questionari che verranno sottoposti dalla compagnia di assicurazioni. Accertarsi di rispondere in modo esaustivo e veritiero. Utilizzarli piuttosto come assessment e come stimolo ad un miglioramento continuo del livello di rispondenza ai più comuni standard di sicurezza;**

→ **Verificare con il broker o altro consulente che la polizza sia adeguata al profilo di rischio e al piano di emergenza. Deve essere in grado di dare effettiva copertura per ciò che occorre in caso di incidente e per tutti i rischi connessi, compresi possibilmente i danni e le sanzioni, i costi forensi e le spese di gestione della crisi;**

→ **Alcune polizze includono servizi di pronto intervento tecnico. Approfondire con i fornitori la natura dei servizi offerti e l'adeguatezza al contesto operativo.**

CONFINDUSTRIA
Varese

IL VOCABOLARIO DELLA SICUREZZA

Antimalware, Antivirus. Sono programmi nati per affrontare i malware e i virus informatici. Rilevano i programmi che generano la minaccia bloccando la loro esecuzione prima che questa abbia causato il danno o cercando di mitigarlo nei limiti del possibile.

Antispam. Sistemi in cloud che intercettano la posta pubblicitaria di basso profilo generalmente indesiderata. Possono intervenire anche sulla sicurezza.

Assessment. Valutazione del rischio informatico effettuata sull'infrastruttura sia a livello tecnologico che di processi.

Autenticazione. Il processo mediante il quale i sistemi verificano l'identità di una persona/organizzazione/applicazione che chiede accesso ad una risorsa. I metodi più diffusi di autenticazione sono le credenziali (username e password o PIN, i certificati digitali, sensori biometrici, smart card, token fisici o App di validazione) che possono essere combinati fra loro per aumentare la sicurezza.

Big Data. Si tratta di un insieme di dati, strutturati o meno, che per quantità, complessità o velocità dei flussi di provenienza, richiedono strumenti, metodi e capacità di analisi particolari. L'analisi dei Big Data può generare molto valore ed è per questo motivo che i venditori di tecnolgia tendono sempre ad inserire "sonde" che poi rendono disponibile una grande quantità di informazioni (spesso legate alla sfera personale) che potranno essere analizzate utilizzate o vendute.

Blacklist. Letteralmente «lista nera». Generalmente un elenco di indirizzi e-mail o IP di mittenti o siti web pericolosi per la sicurezza, utilizzati da sistemi antivirus, antispam o di Cloud Security per bloccare il traffico da essi proveniente o diretto.

Botnet. Una rete di oggetti infetti connessi al web in grado di essere controllati ed attivati da remoto per scatenare attacchi sincronizzati contro obbiettivi designati. Possono far parte di una Botnet: PC, Server, ma anche oggetti interconnessi come telecamere o elettrodomestici wi-fi.

Business Continuity. La capacità di una organizzazione di mantenere la propria operatività, in caso di incidente informatico o altro evento in grado di rendere indisponibili dati e sistemi.

Cloud. Si definisce Cloud tutto il meccanismo di erogazione di risorse (archiviazione o elaborazione) fornito da infrastrutture esterne ed acquistato come servizio scalabile e configurabile.

Cloud Security. L'insieme delle tecnologie e procedure per la sicurezza di dati e infrastrutture in cloud. Definisce anche meccanismi di sicurezza e protezione della navigazione basati su intervento esterno in ingresso e uscita, prescindendo quindi dal luogo fisico da cui si genera il traffico.

Cracker. Persona o gruppo di persone che violando i relativi sistemi di sicurezza guadagnano un accesso non autorizzato ad una risorsa o ad un sistema.

Criptovaluta. Una criptovaluta è una valuta virtuale che costituisce una rappresentazione digitale di un valore, utilizzata come mezzo di scambio o detenuta a scopo di investimento. Le criptovalute possono essere trasferite, conservate o negoziate elettronicamente senza la mediazione di banche centrali o altri organismi di controllo. Le più conosciute sono il Bitcoin, Ethereum, Cardano, Tron. Generalmente le transazioni che riguardano il crimine informatico avvengono tramite l'utilizzo di criptovalute per via della difficile tracciabilità dei movimenti.

Crittografia. Meccanismo matematico attraverso il quale dati archiviati o oggetto di una trasmissione vengono codificati e resi intellegibili solo a soggetti autorizzati in possesso di tecnologia e "chiavi" informatiche necessarie per decodificarli. La cifratura può riguardare indifferentemente file o flussi di dati.

Cryptolocker. Denominazione generica usata impropriamente per definire tutti gli attacchi che cifrano i dati delle vittime per spingerle a pagare un riscatto. In realtà è il nome di uno dei più famosi malware di questo genere, apparso nel 2013.

Cybersecurity. Il complesso delle misure di prevenzione e protezione di tutte le risorse informatiche da minacce di qualsiasi natura come ad esempio furti, calamità naturali, guasti, attacchi informatici, errori umani.

Dark Web e Deep Web. Il Dark Web è una porzione di Deep Web, cioè una parte di www non indicizzato dai motori di ricerca. In particolare il Dark Web è accessibile solo mediante browser specifici e particolari accorgimenti tecnologici che rendono virtualmente irrintracciabile chi naviga e chi pubblica. Per questo motivo, il Dark Web è spesso luogo di attività illecite compresa la vendita di informazioni sottratte con il crimine informatico.

Data Breach. La diffusione o alterazione, dolosa o accidentale, di dati personali. In alcuni casi deve essere notificata all'Autorità Garante entro 72 ore.

Data loss. La perdita definitiva di dati critici (o la loro inaccessibilità a tutti gli effetti) a seguito di un incidente, errori o circostanze non previste. La prevenzione di questo tipo di incidente prende il nome di Data Loss Protection.

Dos o DDos. Attacchi informatici del tipo "Denial of Service" in cui un malintenzionato servendosi generalmente di una Botnet, inonda di richieste una specifica risorsa (ad esempio un sito internet), rendendolo praticamente inutilizzabile.

Disaster Recovery. Si tratta di un progetto di Business Continuity che definisce strumenti e procedure per rispondere in tempi certi ad un grave incidente informatico, garantendo quindi la più rapida ripresa delle attività. Può coinvolgere soggetti esterni all'organizzazione e comportare la stipula di contratti e polizze assicurative.

DNS. È il sistema decentralizzato di risoluzione dei nomi a dominio nel mondo Internet. Una sorta di elenco telefonico che trasforma indirizzi facili da ricordare per gli esseri umani (es. www.confindustriavarese.it) in indirizzi fisici IP (es. 88.149.206.6). Può essere oggetto di attacchi per dirottare la navigazione su siti contraffatti (DNSPoisoning), oppure può essere utilizzato per prevenire il raggiungimento di indirizzi compromesi (DNS Security).

Firewall. Dispositivo o programma software in grado di monitorare e filtrare il traffico di rete. Possono essere posti in corrispondenza della connessione ad Internet dell'organizzazione oppure su singoli terminali.

Hacker. Soggetto o gruppo di persone dedite alla scoperta di vulnerabilità dei sistemi. La definizione non è necessariamente negativa se tali scoperte non vengono utilizzate per commettere crimini.

Impersonificazione. Il complesso delle tecniche attraverso le quali un criminale finge di essere qualcun altro (spesso un VIP) per creare situazioni complesse finalizzate a sottrarre denaro, credenziali o altri dati sensibili. I casi più frequenti si verificano via e-mail ma anche tramite i Social Network più diffusi.

IDS (Intrusion Detection System) – IPS (Intrusion Prevention System). A differenza di un Firewall tradizionale che si basa su liste controllo accessi e regole prestabilite, un sistema IDS controlla dinamicamente il contenuto dei pacchetti in transito e genera un allarme se rileva anomalie secondo modelli prestabiliti. I Sistemi IPS sono invece in grado di bloccare il traffico sospetto in modo automatico.

IoT (Internet of Things). L'insieme di tutti quegli oggetti in grado di connettersi ad Internet esprimendo nuove funzionalità. Ad esempio oggetti domotici, automobili, elettrodomestici...

Mail Merge. La cosiddetta "stampa unione", ovvero la realizzazione di documenti personalizzati utilizzando un testo guida e dei campi variabili, riferiti ad una tabella. In questa guida il termine è utilizzato come suggestione per far capire come sia possibile realizzare una campagna di phishing via e-mail tanto più efficace quanto più sono personalizzati e veritieri i dati utilizzati nella tabella, spesso provenienti da data breach.

Malware. Termine generico per indicare qualsiasi tipo di programma con intenti maliziosi in grado di arrecare danni di qualsiasi tipo, sottraendo informazioni o accedendo illecitamente a sistemi compromettendone la funzionalità.

Man in The Middle – Man in The Mail. Tipologia di attacco molto diffusa per descrivere situazioni nelle quali il criminale informatico si introduce segretamente all'interno di un flusso di comunicazione (ad esempio posta elettronica) carpendo informazioni e documenti che poi utilizzerà per attuare truffe. Spesso questa tecnica viene utilizzata per falsificare fatture inserendo iban in realtà nella disponibilità dell'attaccante.

MDR. Managed Detection & Response. Si tratta di sistemi complessi di monitoraggio continuo della rete di una organizzazione che facendo uso di tecniche predittive e competenze umane è in grado di prevenire o bloccare sul nascere un attacco informatico. Tale funzionalità viene venduta come servizio.

MFA. Autenticazione a più fattori. Inizialmente usata nel mondo bancario, garantisce maggiore sicurezza nell'accesso a risorse a rischio, aggiungendo alle tradizionali credenziali ulteriori meccanismi di validazione come ad esempio codici generati da APP o dispositivi hardware dedicati (token).

Paternità (o non ripudiabilità). Principio secondo il quale ogni documento o processo documentale deve essere associato ad un utente che non deve poter ripudiare o negare ciò che ha firmato digitalmente.

Patch. Letteralmente "pezza". Si tratta di un aggiornamento critico di un programma o di un sistema operativo, che appunto mette una "pezza" a dei problemi di sicurezza o funzionalità. Per tale motivo è estremamente importante che qualunque sistema che lo preveda sia aggiornato con la dovuta frequenza.

Penetration Test (Pen Test). L'insieme delle prove di vulnerabilità di un sistema esposto su una rete. Gli esperti valutano la qualità delle protezioni messe in campo a tutti i livelli e verificano che non vi siano possibilità, allo stato delle conoscenze del momento, di superarle e di prendere il controllo di dati o sistemi.

Phishing. Tentativo fraudolento di ottenere informazioni riservate (generalmente credenziali utente o numeri di carta di credito) ingannando la vittima attraverso indirizzi o siti internet abilmente contraffatti.

Ransomware. Tipologia di malware utilizzato da criminali informatici (spesso gang organizzate) per finalizzare un attacco ad una organizzazione. I dati critici vengono esfiltrati e poi cifrati rendendoli inservibili. Gli attaccanti poi ricattano la vittima richiedendo un riscatto proporzionato alle capacità di spesa, minacciando anche la diffusione dei dati sottratti o altre azioni di vendetta come ad esempio degli attacchi Dos.

RID/CIA. Riservatezza, Integrità e Disponibilità (Confidentiality, Integrity, Availability). Tre parole chiave che racchiudono il concetto di sicurezza informatica che ha quindi il compito di garantire la riservatezza dei dati, la loro integrità e la loro disponibilità al bisogno.

Smishing. Il phishing veicolato attraverso SMS.

Social Engineering. L'insieme delle tecniche psicologiche che spingono la vittima di un attacco a ritenere reale il contesto in realtà contraffatto. Ad esempio un mittente di un'e-mail ritenuto autorevole, un sito perfettamente contraffatto, un SMS ricevuto da un contatto apparentemente reale.

Spoofing. Meccanismo di falsificazione di identità a qualunque livello. Quelli più noti riguardano i mittenti della posta elettronica o di SMS.

Threat Intelligence. La raccolta e l'analisi di informazioni al fine di poter individuare e caratterizzare preventivamente possibili minacce informatiche di qualunque genere in contesti specifici.

Tracciabilità. La possibilità di sapere chi e quando ha agito in lettura, modifica, creazione e cancellazione di un archivio o documento.

VPN. È una tecnologia che permette di raggiungere da remoto la rete interna di una organizzazione facendo uso di credenziali, certificati e crittografia per ridurre il rischio di intrusioni.

Whaling. È una tipologia di attacco phishing mirato espressamente alle alte figure dirigenziali. Facendo leva sul "principio di autorità" o sulla capacità di spesa di questi obiettivi, l'attaccante mira ad ottenere grosse cifre in poco tempo.

Zero-Day. Si tratta di una vulnerabilità non ancora resa nota alla comunità dei tecnici. Può essere utilizzata per anni da diversi soggetti (tra cui agenzie di spionaggio o forze dell'ordine) per intercettare informazioni, oppure essere la porta di ingresso di attacchi improvvisi su larga scala prima che sia disponibile una patch per sanarla.

CONFINDUSTRIA
Varese

Pubblicazione realizzata dal Gruppo Merceologico
"Terziario Avanzato" di Confindustria Varese
nell'ambito del Progetto "PuntoZero - un percorso di avvicinamento
alla Sicurezza Informatica nelle imprese".

A cura dell'Area "Sistemi Informativi" di Confindustria Varese.

Grafica e impaginazione: Paolo Marchetti

Edizione Ottobre 2021

www.confindustriavarese.it/puntozero

CONFINDUSTRIA Varese

Gruppo Merceologico "Terziario Avanzato"

I nostri Social

Varesefocus

ConfindustriaVarese

Confindustria Varese

ConfindustriaVarese

Buongiorno Impresa e
News d'Impresa