Nowtech

Sicurezza Informatica

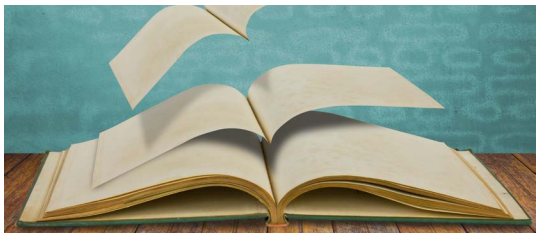
i temi chiave

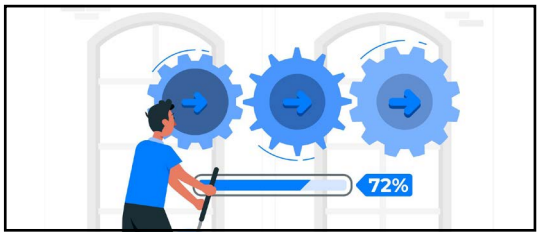
strumenti
indispensabili
per la tutela
della Tua azienda

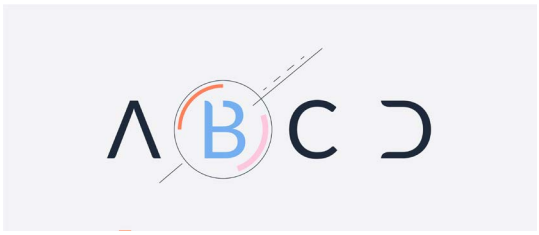
I TEMI DELLA CYBER SECURITY COME CHIAVE PER SVILUPPARE UNA CONSAPEVOLEZZA SULLA SICUREZZA INFORMATICA PERSONALE E DI IMPRESA

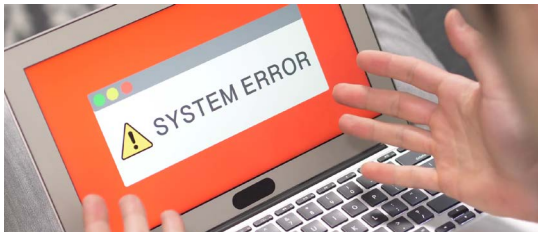
“Così tra questa immensità
s'annega il pensier mio:
e il naufragar m'è dolce in questo mare”
Giacomo Leopardi

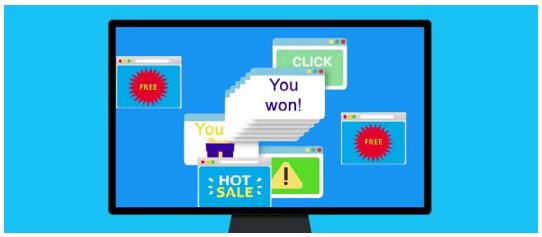
Indice contenuti

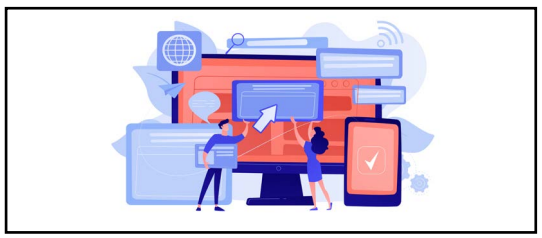


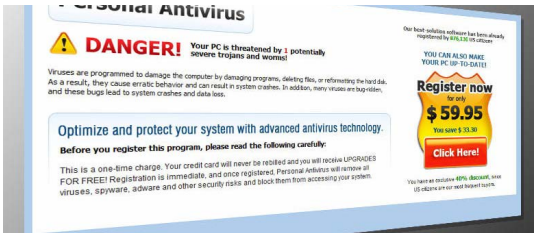


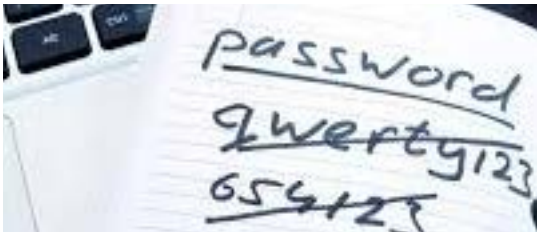












PERCHÈ
QUESTO E-BOOK

Internet è **interazioni ed interconnessione tra utenti,** è **vita reale**. Ma ci ostiniamo ad usarla come se fosse un mondo a parte, e dal quale non possono derivare problemi.

Usciremmo senza chiudere a chiave la porta di casa o dell'azienda? Guideremmo in un quartiere malfamato con finestrino aperto, braccio fuori e oggetti d'oro in bella vista? Seguiremmo un losco figuro in un vicolo buio, che vuole proporci un affare?

Probabilmente no... ho indovinato?

E allora perchè ci ostiniamo a usare password elementari per i nostri account, clicchiamo su banner pubblicitari equivoci, e ci colleghiamo alla prima rete Wi-fi non protetta che captiamo con lo smartphone?

Nella vita reale abbiamo imparato quali comportamenti possono esporci a rischi, ce lo hanno insegnato fin da bambini. I comportamenti da tenere su internet, invece, non ce li hanno insegnati, andiamo ad intuito e a volte questo ci trae in inganno. Spesso abbiamo imparato a nostre spese, attraverso l'esperienza, dopo che il danno è stato fatto.

Vogliamo risparmiarvi un po' di danni.

Ecco un elenco di temi a cui prestare attenzione, e i consigli su **Come Difendersi.**

LA SICUREZZA È UN PROCESSO SISTEMICO

Chiarire le necessità della sicurezza informatica è fondamentale per l'efficienza aziendale

Le aziende, il più delle volte, sottovalutano l'aspetto sicurezza informatica, quando basterebbe semplicemente un po' di buon senso nel dedicare un piccolo lasso di tempo alla formazione del personale per far comprendere a tutti le problematiche principali che la riguardano.

Oggi esiste la necessità di creare politiche sulla sicurezza non troppo complicate per gli utenti e abituare l'utente "distratto" ad aver maggior attenzione nelle attività quotidiane.

La sicurezza parte sempre da una corretta percezione dei rischi da parte dei dipendenti impegnati nell'utilizzo dei sistemi aziendali. Quindi è fondamentale formare correttamente tutti i dipendenti dell'azienda al fine di minimizzare i rischi connessi alla sicurezza dell'azienda stessa.

Al giorno d'oggi non ci si rende conto di come i dati siano facilmente accessibili in rete e di come sia facile trovare informazioni importanti semplicemente navigando. **Gli obiettivi degli hacker vanno dalla ricerca di vulnerabilità dei sistemi alla ricerca di vulnerabilità della persona.**
È importante che tutti siano informati sul concetto della sicurezza per aver maggior consapevolezza dei rischi cui si va incontro.

Delia Scognamiglio

CONSAPEVOLEZZA NEI PROCESSI AZIENDALI

Se siamo consapevoli evitiamo spiacevoli incontri

A mano a mano che i mercati si espandono, aumentano i rischi e le probabilità di incorrere in spiacevoli "incontri". I cybercriminali si sono specializzati ad effettuare campagne email mirate, lanciate attraverso l'utilizzo di tecniche all'avanguardia e sfruttando spesso temi di interesse comune, così come si è visto negli ultimi mesi in cui il tema del Coronavirus è stato oggetto di diversi attacchi rilevati dai nostri esperti. La **Nowtech** lavora per far crescere la consapevolezza delle aziende sulle minacce informatiche e sui rischi a cui andiamo incontro. Studiamo e proponiamo soluzioni di cybersecurity misurate sulle specifiche esigenze di business dei nostri clienti. Siamo consapevoli che ogni settore ha le sue specifiche esigenze e ci sforziamo di mettere a disposizione di ogni settore le misure più efficaci ed economiche per migliore efficienza e sicurezza. I nostri obiettivi principali sono: aumentare la sicurezza informatica all'interno delle organizzazioni; incoraggiare i responsabili aziendali a condividerne l'importanza con tutte le parti aziendali e a gestirne l'applicazione. Solo se tutte le parti aziendali lavorano insieme, l'obiettivo dell'implementazione può avere successo.

Per questo abbiamo lavorato a questo libro, il primo di una collana di approfondimenti che crediamo possa aiutare i responsabili dell'informatizzazione e ogni dipendente ad aumentare la sua consapevolezza sui temi della sicurezza.

Antonio Aprea

ETICA ED INNOVAZIONE

Impegni e responsabilità

Tra le tante sfide degli ultimi anni, la Nowtech si impegna non solo a proteggere i suoi dati ma avendo numerose relazioni con Clienti e Fornitori, si preoccupa anche e soprattutto di salvaguardare i dati di quest'ultimi.

Essere responsabili per noi significa mantenere tale impegno verso i nostri stakeholder perché è in momenti come questi che emergono le vere differenze tra chi parla solo di GDPR perché va di moda e chi, come noi, pratica questo approccio da quasi trent'anni, in quanto è il nostro modo di essere. E questo chi lavora con noi lo sa. Auspico che chi invece ci conosce meno lo percepisca dalla lettura di questa pubblicazione.

L'attenzione al GDPR quindi è intensa, non solo a livello interno ma anche a livello esterno. Questo impegno contribuisce alla protezione con riguardo al trattamento dei dati personali di tutti gli stakeholder e a contenere fortemente il rischio di perdita di reputazione nei loro confronti.
Da sempre infatti la filosofia aziendale combina l'attività imprenditoriale e innovazione grazie ad un continuo lavoro di miglioramento da parte del nostro personale dotato di una forte motivazione professionale.

Lisa Di Tuccio

OCCHI APERTI!

Basta un semplice click sull'allegato sbagliato

I virus informatici provocano danni enormi, sopratutto a causa della scarsa conoscenza da parte delle vittime, si pensi alle terribili conseguenze che può generare un semplice click sull'allegato sbagliato.

Lo scopo di questo eBook è una maggiore consapevolezza del rischio informatico.
Nella maggior parte dei casi siamo noi stessi, inconsapevolmente ad aprire le porte della nostra banca dati o del nostro archivio sul computer.
Nonostante il tema della sicurezza informatica sia ormai da tempo al centro dell'attenzione, non vengono ancora adottati i corretti comportamenti che ci evitino di cadere in trappola.
Così come ci preoccupiamo di installare allarmi e porte blindate per proteggerci dai ladri nel mondo reale, così dovremmo occuparci della protezione dei nostri dispositivi e dei dati in essi contenuti.

Le minacce con le quali combattiamo quotidianamente hanno nomi particolari come malware, keylogger, bot, rootkit, spyware, trojan, virus, worm, etc... e questo per chi non è un esperto complica le cose. Ma non temere, con questo breve libro, insieme cercheremo di fare chiarezza. Sei pronto ad iniziare il viaggio nel mondo dei rischi informatici? Bene, Andiamo!

Ernesto Romano

GLOSSARIO

Se ti conosco ti evito (o mi difendo)

Abbiamo messo insieme un elenco delle minacce con le quali combattiamo quotidianamente, tanti termini sono associati a tecniche sofisticate di attacco e possono causare notevoli problemi andando ad intaccare i nostri risparmi o la nostra reputazione.

Le minacce possono provenire essenzialmente da due strumenti: i malware e i virus.

Cos'è un malware?
"malicious software", ovvero "software maligno" si riferisce a qualsiasi programma creato per effettuare un'azione non autorizzata che può danneggiare il funzionamento e la sicurezza dei nostri device e dei nostri dati. Si trasmette principalmente via internet, tramite la posta elettronica o la semplice navigazione su un sito web, ma possiamo inciamparci anche usando chiavette USB non sicure.
La famiglia dei Malware è estremamente folta e sono molti i tipi da cui dobbiamo guardaci.

Cos'è un Virus?
E' un programma che si propaga di file in file all'interno di uno stesso PC e da un PC all'altro, e può essere programmato per cancellare o danneggiare dati. Spesso è mascherato all'interno di programmi che sembrano innocui.

Account: È l'insieme dei dati che identificano un utente come persona autorizzata ad accedere a un servizio informatico.

Adware: software che genera la presentazione di messaggi pubblicitari (spesso tramite banner pop-up) o reindirizza a siti promozionali non richiesti. Spesso è contenuto all'interno di programmi gratuiti, oppure può essere scaricato ed installato da un Trojan. L'Adware può anche modificare le impostazioni del browser e reindirizzare la navigazione verso un sito specifico.

Binder: Questi programmi servono per unire il Malware ad un programma secondario, in genere viene usato per non far sospettare l'utente dopo aver aperto il Malware, se sta scaricando un file convinto che sia uno screensaver del Film Star Wars o Gioco preferito, quando lo eseguirà si aprirà lo screensaver, ma anche il Malware.

Botnet: Questo è il tipo di strumento che utilizzano gli hacker per crashare e mandare offline i server, è possibile definire una botnet come un punto dove convergono tutte le vittime che l'hacker può gestire comodamente con un pannello, viene spesso associato ad altri Malware per aumentarne la distribuzione, vengono definiti spesso come trojan più sofisticati. Una volta che questo tipo di Malware viene eseguito su un computer, automaticamente questo diventa parte di una rete di bot, che l'hacker può utilizzare per effettuare attacchi ddos, ossia convergere tutte le vittime della botnet su un solo obiettivo con l'intento di far andare in crash il server.

Backdoor: in inglese significa porta sul retro o di servizio. In ambito informatico, una backdoor è una porta di accesso a un sistema informatico che consente a un utente remoto di controllarlo. Alcune backdoor sono progettate da sviluppatori di software e svolgono funzioni utili per gli utenti, come i programmi legittimi di gestione remota, ad esempio TeamViewer. Purtroppo però, le backdoor sono più conosciute per le applicazioni di tipo criminale, ovvero quando la backdoor viene creata da un hacker per accedere illegalmente al sistema di una vittima.

Cookie: letteralmente significa "biscotto" vengono utilizzati dalle applicazioni web lato server per archiviare e recuperare informazioni a lungo termine sul lato client.

Cracker: Dall'inglese "to crack", rompere. Il cracker è per definizione l'hacker "cattivo", quello che sfrutta la sua abilità tecnica per introdursi nei computer/sistemi informativi altrui a scopo criminale.

Crimeware: Software maligno installato di nascosto sui computer degli utenti, con lo scopo principale di "rubarne" informazioni riservate e procedere a una frode online. La maggior parte del crimeware è composta da Trojan.

DOM Storage: (Document Object Model storage) è un modo per i siti web di memorizzare informazioni sul computer dell'utente e recuperarle più tardi. Il concetto è simile a quello dei cookies, con la differenza che è stato concepito per grosse quantità di informazioni.

Hacker: Persona dotata di notevoli conoscenze tecniche, che gli permettono di investigare in profondità sul comportamento di un sistema informatico, alla ricerca di difetti e vulnerabilità. A differenza del cracker, l'hacker generalmente è mosso soprattutto dalla voglia di conoscenza e dalla curiosità, e comunque non agisce per scopi illeciti; anzi, tipicamente quando scopre vulnerabilità in un sistema provvede a informare i programmatori del problema, spesso suggerendo anche il modo per risolverlo.

Keylogger: si tratta di programmi che registrano tutto ciò che l'utente digita sulla tastiera, nella maggior parte dei casi sono progettati per rubare dati sensibili quali login, password e codici bancari. Il funzionamento di un Keylogger software è abbastanza elementare, sono facili da usare e per questo rappresentano il Malware più usato da chi inizia a mettere piede nel mondo dell'hacking.

Logging bomb: Una bomba logica è un malware che è in grado di modificare o cancellare i file al verificarsi di una condizione. Inizialmente si presenta come innocuo fino al verificarsi di alcune condizioni particolari (ad esempio quando viene superata una dimensione di dati sull'hard disk).

Ransomware: La parola deriva da Ransom che in inglese significa riscatto. Un tipico Ransomware limita l'accesso ai i file contenuti nel proprio PC. Viene usato come leva per chiedere un "riscatto" in cambio del programma necessario a sbloccare il nostro computer, rimuovendo le limitazioni imposte dal programma malevolo.

Rootkit: è un programma che permette di accedere a un computer senza l'autorizzazione dell'utente o dell'amministratore. Una volta installato è invisibile agli utenti e riesce ad eludere anche i software di sicurezza.

Scareware: sono dei software dannosi che se installati sul

computer possono fornire false informazioni agli utenti, convincendoli ad acquistare dei programmi.

Stealers: Sono un tipo di Malware molto comune, il loro unico scopo è rubare tutte le password salvate nel tuo computer e inviarle via email o caricarle sullo spazio FTP dell'hacker, in genere vengono rubate tutte le password che scegliamo di far ricordare al browser, spuntando la casella "Ricorda la Password".

Spoofing: tipo di attacco informatico che impiega in varie maniere la falsificazione dell'identità.

Spyware: Gli spyware spiano abitudini e informazioni della vittima per recapitarle all'hacker.

Trojan: il nome deriva dal Cavallo di Troia. Come il Cavallo di Troia è stato un dono contenente una minaccia, così il Trojan è un malware nascosto in un programma che appare come un software innocuo ma che, una volta lanciato, danneggia o compromette la sicurezza e il funzionamento del computer.

VPN: il termine identifica una Rete Virtuale Privata (**V**irtual **P**rivate **N**etwork). Rete e intesa come **Privata perché per accederci bisogna avere un account con delle credenziali** (tipicamente username e password) e **Virtuale perché viene creato un ponte di connessione Virtuale** tra chi si connette e uno dei server della rete. Una delle caratteristiche di questo tipo di connessione sono spesso la criptazione dei dati durante la trasmissione e il ricevimento. Un esempio di VPN è un ufficio che permette ai propri dipendenti o agenti di connettersi, per poter lavorare come se fossero in ufficio.

Worm: sono particolari tipi di virus che, per diffondersi utilizzano la rete. Si installano in un computer per poi trovare il modo di diffondersi ad altri PC.

CYBER SECURITY

Una pratica da applicare in qualsiasi contesto informatico

La **Cyber Security** è la pratica che si occupa della protezione dell'informazione e dei sistemi informatici da attacchi digitali interni ed esterni. Nella Cyber Security sono coinvolti fattori tecnici, organizzativi, giuridici e umani.
Molti utenti non sono in grado di riconoscere i pericoli derivanti dai loro inconsapevoli comportamenti e vi cadono facilmente vittima, mettendo in pericolo la sicurezza dei loro dati e di quelli aziendali.

Per valutare la sicurezza è solitamente necessario individuare le minacce, le vulnerabilità e i rischi associati agli asset informatici (PC, Server, Telefoni IP, Router, ecc...), al fine di proteggerli da possibili attacchi che potrebbero provocare danni diretti o indiretti di impatto superiore a una determinata soglia di tollerabilità di un'organizzazione.
Le minacce ai dati possono anche derivare da persone esterne quali tecnici, clienti, fornitori o semplici ospiti che accedano alla rete aziendale tramite computer o altri dispositivi portatili, ad esempio tramite Wi-Fi. Ancora peggio, se tramite un computer di un utente lasciato incustodito e non bloccato da una password.

La definizione cyber security seppure spesso tradotta con il concetto di sicurezza informatica, non è esattamente rappresentato dalla traduzione in italiano. Il concetto espresso in inglese contiene aspetti concernenti sia la protezione dagli attacchi, sia quella della protezione da incidenti o guasti. **Gli attacchi e le minacce mirano a creare confusione** tra due aspetti, in modo da rendere difficoltoso il ripristino delle normali attività.

Per garantire alti livelli di efficienza ed evitare le interruzioni derivanti da queste minacce, vanno utilizzati diversi strumenti: antivirus, software di monitoraggio hardware, controlli periodici sulle password degli account e sistemi di backup. La reale tutela nel mondo digitale avviene soprattutto adottando comportamenti consapevoli che ci eviteranno di cadere nei tranelli ai quali questa nuova dimensione ci sottopone quotidianamente.
Nelle pagine che seguono cerchiamo di approfondire alcuni temi di questo complesso mondo della sicurezza.

L'ANELLO DEBOLE

il fattore umano

Nell'ultimo anno abbiamo vissuto una vera e propria trasformzazione delle nostre vite. E'cambiato il nostro modo di lavorare, di fare relazione, di pensare ed organizzare il nostro tempo. La società intera ha subito una forte spinta verso il digitale, evidenziando sia le grandi possibilità che i rischi e le minacce sempre più pressanti. Abbiamo sperimentato nella pratica che non eravamo pronti ad utilizzi così massivi della rete e delle sue infrastrutture. E' emerso con prepotenza quanto il fattore umano sia diventato centrale nella gestione dei processi, e quanto sia diventato importante investire su di esso per aumentare la consapevolezza e le capacità di intervento degli operatori e dei dipendenti, per garantire alti livelli di sicurezza ed efficienza.

Il problema non riguarda solo le persone meno abituate all'utilizzo delle tecnologie digitali, ma anche le nuove generazioni e i cosiddetti **"millennials"**. Lo studio sulla generazione Y che Mark Prensky definisce "nativi digitali" si evolve con le considerazioni di Anna Rita Longo su Scientificast che aggiunge alle definizione nativo digitale quella di "Nativi ed analfabeti digitali". E' il paradosso delle generazioni google. E' proprio questa, che pur avendo una naturale propensione all'uso delle tecnologie, mostra i comportamenti degli **"utenti inconsapevoli";** che dimostrano una profonda incapacità di riconoscere quelli che sono i rischi collegati alle loro azioni.

Per usare la metafora bellica, nella guerra contro i cybercrimini chi attacca è in una posizione di vantaggio poiché s la prima linea di difesa è costituita da civili "inermi" che non hanno la sufficiente consapevolezza delle minacce e delle contromisure necessarie a difendersi.

L'esperienza degli scorsi anni ci ha fatto comprendere quanto sia centrale il fattore umano in tutta la catena della sicurezza. Le aziende e le grandi organizzazioni hanno investito molto, anzi moltissimo, sugli "apparati" tecnologici di sicurezza, che frequentemente sono stati neutralizzati dalla mancanza di consapevolezza e di preparazione del personale aziendale. Il fattore umano rischia di vanificare lo sforzo economico! Ecco perché la battaglia appare come squilibrata in favore di chi attacca.

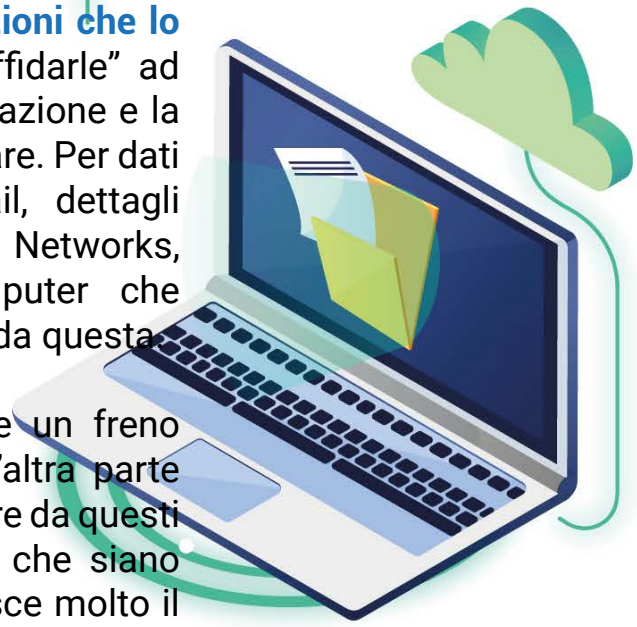
Per portare speranza in queste battaglie giornaliere **è necessario che gli utenti acquisiscano consapevolezza,** per maturare abitudini e adeguare i propri comportamenti rispetto ai rischi Cybernetici. Un processo continuo possibile solo con l'acquisizione di conoscenze teoriche e di **formazione continua nei diversi ambiti di applicazione**. Un percorso di formazione rivolto ad aumentare la percezione del rischio, proveniente da un "mondo" non percepito come reale.
Questi processi sono misura necessaria per le organizzazioni di oggi, ma **devono diventare sistemici** per la creazione di una generazione di utenti consapevoli ed evoluti capaci di utilizzare le enormi potezialità offerte dalla tecnologia, ed allo stesso tempo difendersi efficacemente.

Nella Cybersecurity il fattore umano è decisivo. Rafforzarlo significa dare rafforzare l'anello debole.

Il General Data Protection Regulation

Regolamento Generale sulla Protezione dei Dati

Il GDPR è l'acronimo di **G**eneral **D**ata **P**rotection **R**egulation, ed è il regolamento dell' Unione Europea in materia di trattamento dei dati personali. E' entrato in vigore il 24 maggio 2016, ma la sua attuazione è avvenuta a distanza di due anni, quindi a partire dal **25 maggio 2018**. L'azione della comunità Europea introduce un concetto originale. **Ogni individuo è il vero titolare delle informazioni che lo riguardano** e può liberamente decidere di "affidarle" ad altri, in un ambito di trasparenza sulla conservazione e la gestione che il titolare del trattamento ne può fare. Per dati personali si intende: Nomi, Foto, Indirizzi, email, dettagli bancari, Interventi su siti web e sui Social Networks, Informazioni mediche, Indirizzi IP di computer che caratterizzano la nostra persona in rete e fuori da questa.



Così, la nuova normativa sulla Privacy mette un freno all'utilizzo spregiudicato dei dati personali. D'altra parte spinge chi rilascia i propri dati a terzi a pretendere da questi di produrre e proporre strumenti e garanzie che siano sicuri e facili da usare anche da chi non conosce molto il mondo informatico.

E’ stato certamente un passaggio che ha cambiato radicalmente il modo di concepire i dati personali, responsabilizzando sia chi li tratta che chi li concede. I primi attraverso l’istituzione di solide politiche di sicurezza informatica e per i secondi accrescere la consapevolezza che le azioni sui dati se non correttamente eseguite, possono avere una ricaduta anche al di fuori del web.

Il nuovo regolamento, in conclusione, tutela il diritto alla libertà di ognuno sulla gestione dei propri dati personali, piuttosto che obbligare ad una generica riservatezza alla quale erano soggetti in passato i titolari del trattamento.
E’ a questa libertà, conseguita grazie al consapevole utilizzo dei nostri dati, che miriamo con la redazione di questo ebook.

La quantità di dati che conserviamo nei nostri dispositivi è impressionante.

PROTEGGILI!

A molti truffatori potrebbero tornare utili.

INGEGNERIA SOCIALE

Come sfruttare i punti deboli dell'uomo

Gli specialisti informatici si occupano di garantire la sicurezza Informatica, ma **spesso le vulnerabilità maggiori non si trovano nella rete, bensì a 40 centimetri dallo schermo,** dove gli utenti in carne e ossa interagiscono con la tecnologia. I truffatori lo sanno molto bene, infatti sfruttano le tipiche qualità dell'uomo e i comportamenti più comuni come la fiducia nel prossimo, la disponibilità, il rispetto, la fierezza, la riconoscenza, l'evitare i conflitti o la paura, tutto per riuscire ad avere accesso illegalmente ai sistemi dei malcapitati, usando il metodo dell'ingegneria sociale, che provoca ogni anno miliardi di danni. Quindi per le aziende è indispensabile riuscire a sensibilizzare i lavoratori su questo tema ed avere delle chiare linee guida per sapere come gestire le informazioni confidenziali.

Che cos'è l'ingegneria sociale?
L'ingegneria sociale è composta da diversi trucchetti psicologici, per strappare ai lavoratori informazioni importanti. Si utilizzano queste tecniche per infiltrarsi nei sistemi informatici e avere accesso ai dati sensibili di un'azienda: si parla così anche di social hacking. L'ingegneria sociale viene utilizzata per indurre i dipendenti ad azioni sconsiderate, come ad esempio l'installazione di un programma sconosciuto o transazioni finanziarie sospette. Normalmente non è richiesto un contatto diretto tra il truffatore e la vittima. Anche le email di phishing che mirano a ingannare gli utenti, si basano la maggior parte sull'ingegneria sociale.

> Anche la password più sicura offre poca sicurezza, se è detta mentre si parla con gli sconosciuti

Un classico esempio è ricevere una mail di un presunto amministratore di sistema a cui serve la password della segreteria per risolvere velocemente un problema improvviso.

Come funziona l'ingegneria sociale?

L'idea dell'ingegneria sociale sembra banale, ma si dimostra nella pratica uno dei metodi più efficaci di infiltrazione perché fa leva sulle caratteristiche positive e negative, che si trovano in quasi tutte le persone. Molte persone hanno difficoltà a rifiutare di fare un favore in una situazione di emergenza e per paura di reagire in modo sbagliato in situazioni sconosciute, molti decidono di collaborare.

Ma non sono sempre le qualità dell'uomo ad essere al centro dei tentativi di manipolazione. Spesso la tendenza ad evitare conflitti comporta che vengano eseguite azioni poco sicure contro ogni buon senso. La paura invece fa compiere azioni avventate, come ad esempio quella di fornire informazioni dettagliate sul router e sulla sua configurazione ad un presunto tecnico al telefono che prospetta un pomeriggio senza Internet. Chiamate di questo tipo intimidiscono soprattutto i lavoratori con poche conoscenze informatiche perché sono piene di termini tecnici a loro sconosciuti. I **social hacker** si approfittano anche della paura dei superiori, infatti un tipico trucco è fingere un ordine di pagamento da parte del capo.

Per ingannare le loro vittime, i truffatori si fingono solitamente colleghi, superiori o candidati. Gli hacker si fingono impiegati del servizio che deve raccogliere informazioni sul grado di soddisfazione dei clienti o che deve condurre per conto di un istituto di ricerca un sondaggio del settore.

I così chiamati ingegneri sociali non si limitano necessariamente ad un unico contatto. È possibile che comincino con chiedere alcuni piccoli favori o continuare a farsi risentire di tanto in tanto. Il tentativo di hacking vero e proprio avviene solo quando si è instaurato un certo

rapporto di fiducia e l'hacker ha raccolto le informazioni necessarie per poter ingannare la vittima facilmente. Tra le possibili fonti di informazione rientrano, oltre alla pagina aziendale, i social network come Facebook o LinkedIn e alcuni criminali si spingono addirittura molto oltre con il **dumpster diving**, ricercando nel cestino della vittima documenti di lavoro buttati senza pensarci troppo.
L'ingegneria sociale per e-mail o per telefono è molto comune perché permette l'automatizzazione di questi attacchi con pochi accorgimenti tecnici. Il rischio di rivelare inavvertitamente segreti aziendali o dati di accesso esiste anche nei mezzi pubblici o in luoghi come bar, ristoranti o locali, quando più colleghi conversano in un'atmosfera rilassata sui numeri, i processi o i contatti dell'azienda. Anche i dipendenti che hanno conversazioni di lavoro al telefono discutono spesso di informazioni riservate alla luce del giorno e senza preoccuparsi di possibili ascoltatori.

Software per l'Ingegneria sociale automatizzata

Una variante dell'ingegneria sociale basata su un software si appoggia su programmi dannosi specifici, che impauriscono gli utenti e li inducono così a compiere precise azioni: si parla in questo caso di **scareware**. I programmi di questo tipo seguono questo schema: gli utenti vengono informati da un software su una specifica minaccia e gli viene mostrata allo stesso tempo una semplice soluzione, che comprende in genere l'azione voluta dall'hacker. Spesso lo scareware viene posizionato prima sul computer della vittima. Un punto di appoggio è offerto qui dalla fiducia riposta in marchi conosciuti, aziende o istituzioni. Per invogliare l'utente ad installare spontaneamente un malware, i truffatori usano, tra gli altri, nomi e loghi che si confondono facilmente con prodotti famosi affidabili.

Così uno scareware si può ad esempio nascondere in un programma antivirus gratuito, che comunica all'utente, dopo l'installazione, una serie di infezioni fittizie e offre come soluzione al problema il download della versione completa a pagamento.

L'uso di scareware non prevede necessariamente un'infiltrazione nel sistema, ma può anche iniziare ad esempio tramite un'animazione su un sito, che fa credere alla vittima di aver subito un attacco hacker. Le "misure di sicurezza" offerte dallo scareware comprendono in questo caso il download di un trojan, che consente poi l'attacco vero e proprio. In una variazione di questo schema di attacco il messaggio di errore non viene mostrato sul sito, ma viene semplicemente attivato come un avviso del browser. Sono anche possibili delle finestre pop-up, che imitano i conosciuti avvisi del sistema di Windows.

Come tutelarsi in azienda

Per proteggere efficacemente la propria azienda dall'ingegneria sociale, bisogna sensibilizzare i dipendenti partendo da quelli che sono in possesso di informazioni riservate. Inoltre si consiglia di stabilire delle regole per procedere con i dati aziendali sensibili. I procedimenti standard per compiti amministrativi danno sicurezza ai lavoratori e indicano come ci si dovrebbe comportare in caso di situazioni critiche. Se ai dipendenti viene suggerito di non chiedere mai password personali dell'azienda per e-mail o al telefono, sarà difficile per i truffatori avervi accesso tramite uno di questi canali.
Visto che l'ingegneria sociale si basa sull'errore umano, non è possibile eliminare del tutto il rischio solo ricorrendo a misure preventive.

- Diffidare di persone che non fanno parte dell'azienda, più un'azienda è grande, più è facile per persone non appartenenti all'azienda, dire di essere dei lavoratori o dei fornitori. Di solito diffidando degli estranei diminuisce il rischio di rivelare informazioni riservate dell'azienda, infatti si dovrebbero fornire dati sensibili solo ai colleghi,

la cui identità è nota. Mai dare informazioni sensibili al telefono, soprattutto nel caso si tratti di telefonate in entrata o di interlocutori sconosciuti. Anche informazioni apparentemente secondarie possono aiutare i truffatori a raccogliere informazioni sull'azienda e trarre magari in inganno altri colleghi.

- Di Fronte ad un'email con mittente sconosciuto o non chiaramente identificabile, si consiglia di procedere con cautela. I lavoratori dovrebbero consultare in ogni caso il reparto IT, prima di rispondere a messaggi simili. Se nel messaggio viene richiesto il compimento di un'azione inaspettata, ad esempio si chiede di effettuare eccezionalmente un bonifico, si consiglia di chiamare il presunto mittente per verificare la situazione.

- Cautela nel cliccare sui link e nell'aprire gli allegati delle e-mail. I truffatori utilizzano tecniche di questo tipo per ottenere dati bancari, password o codici cliente.

Ai dipendenti dovrebbe essere chiaro dove è possibile utilizzare e salvare i dati sensibili e quali informazioni dovrebbero in ogni caso rimanere segrete

- Si consiglia sempre di stare attenti ad aprire gli allegati, perché possono contenere malware, che si installano a vostra insaputa, fornendo accesso al sistema a persone non autorizzate. È possibile ridurre questo rischio, esortando i dipendenti ad aprire solo allegati alle e-mail di mittenti conosciuti.

- La preparazione di attacchi di ingegneria sociale avviene generalmente molto prima rispetto all'attacco vero e proprio. Oltre al sito aziendale, anche i social network offrono spesso ai truffatori informazioni sufficienti per confezionare i loro tentativi di manipolazione in una storia credibile. Generalmente vale il fatto che più un dipendente fornisce informazioni su di sé in rete, più si espone ai rischi dell'ingegneria sociale diventando un facile bersaglio. Per questo bisognerebbe informare i dipendenti e stabilire delle chiare regole su come procedere per i contenuti relativi all'azienda sui social network.

La complessità del tema e la varietà degli schemi di attacco rendono però impossibile per i dipendenti essere preparati a tutti i possibili tipi di attacchi di ingegneria sociale.

Tenere regolarmente corsi sulla protezione dei dati aiuta a riportare l'attenzione su questo tema e crea una maggiore consapevolezza dei potenziali rischi.

Comunque, attenzione a non esagerare con le misure di prevenzione, può diventare difficile ottenere una collaborazione proficua, se si lavora in un clima dove regna una costante paura di sbagliare e diffidenza generale nei confronti degli altri.

Banche, negozi online seri o istituti assicurativi non richiedono ai clienti di aprire un sito e di inserirvi i loro dati sensibili

COME DIFENDERSI

.01
Fermatevi a pensare
I social engineer vogliono che agiate subito e pensiate dopo. Se riceve-te una telefonata o una email che trasmette urgenza e pressione siate scettici.

.02
Verificate sempre
Siate sospettosi di ogni messaggio ricevuto soprattutto se non richies-to. Utilizzate i motori di ricerca per verificare le informazioni e fonti.

.03
Diffidate dagli Sco-nosciuti
Non fidatevi delle richieste perve-nute via email. Anche le email di mittenti conosciuti (amici) possono essere falsificate (spoofing).
Non comunicate dati sensibili a sconosciuti sia al telefono che di persona.
Se un estraneo vi chiama dal tele-fono di un vostro amico o familiare e vi chiede informazioni riservate siate diffidenti!

.04
Occhio ai Social
Comunicate il minor numero pos-sibile di informazioni personali su di voi. Sui siti di social networking come Facebook, Instagram, ecc., in particolare, è opportuno agire con grande cautela nella pubblicazione di informazioni.

.05
Protezione per ac-cesso al PC
Non lasciate mai il vostro PC senza una protezione da password.

.06
La password è per-sonale
Le password non vanno mai comu-nicate a un’altra persona. Nemmeno a un amministratore di sistema o al vostro capo. La password appar-tiene solo e soltanto a voi!

I BIG DATA

Il nuovo petrolio

Si scrive Big Data ma si legge: ”la più grande rivoluzione del nostro tempo”. Non stiamo esagerando, è la più grande rivoluzione perché questo nuovo modo di concepire le informazioni ha ricadute su ogni ambito della società e dell’individuo. Nulla è escluso, politica sanità, acquisti individuali, suggerimenti di programmi televisivi che rispecchiano i nostri gusti. Tutto ciò che ha a che fare con il singolo individuo e con la società nella quale è inserito.

Facciamo un passo indietro. Ogni minuto centinaia di milioni di persone sono collegati con i loro dispositivi alla rete internet. Ognuno di essi esegue delle operazioni (cercare sui motori di ricerca, popolare social, acquistare cose, informarsi attraverso news e giornali online…), queste operazioni sono dati singoli che gli algoritmi leggono riconoscono e organizzano in insiemi di dati. Questi insiemi di dati grezzi sono il territorio preferito da analisti finanziari, politici, esperti di marketing, sociologi e programmatori di intelligenze artificiali. Facciamo un esempio, molto calzante in questo periodo così speciale.

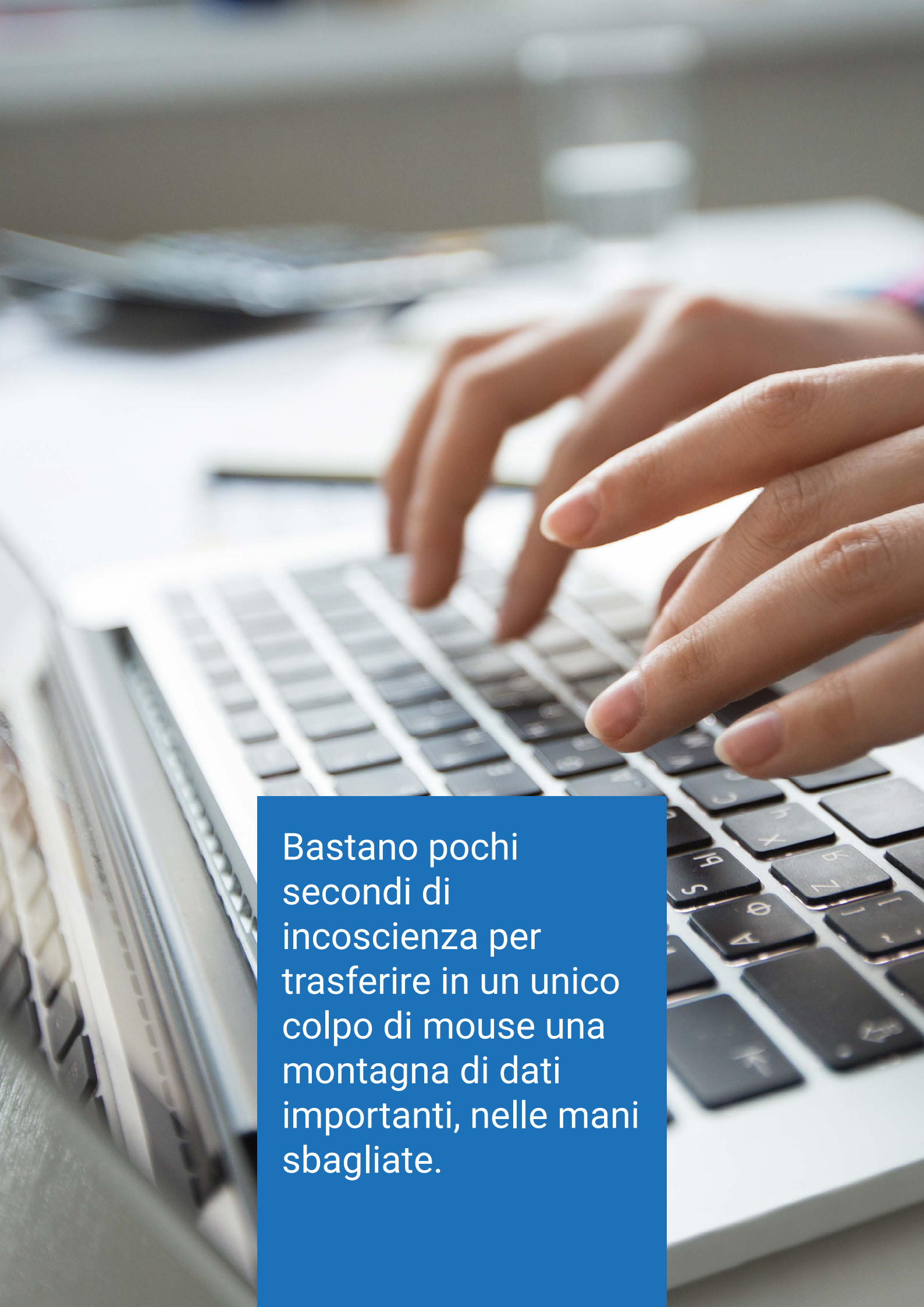
Il progetto condotto da Google. Moutain View, analizzando i gruppi dei termini di ricerca digitati dagli utenti sul proprio motore, era riuscito a prevedere (solo nel 2008) l’avanzamento dei focolai di influenza nei territori degli USA più velocemente di come lo stesso ministero della salute non fosse riuscito a fare utilizzando i record di ammissione ospedaliera delle strutture sanitarie pubbliche e private.

Non si tratta di fantascienza, è solo il presente… anzi in questo caso è il passato che conferma il presente ed annuncia il futuro.

Più che uno strumento i Big Data sono un modo nuovo di gestire e usare le informazioni, una modalità resa possibile dalla grande velocità di calcolo che i computer hanno raggiunto. Solo 30 anni fa questo era impossibile, se non con macchine grandi quanto una stanza e costose come un attico al centro Napoli. Oggi basta un portatile e una connessione ad una delle migliaia di banche dati per usufruire di questa enorme mole di informazioni. Ecco perchè sono diventati così importanti, ed ecco perchè le nostre informazioni sono diventate così preziose. Ecco perché i centri di raccolta di questi dati sono continuamente sotto attacco. Secondo ANSA, nel 2020 sono state 49 mila le organizzazioni pubbliche e private nel mondo, ad aver subito il furto, o il tentativo di furto, delle loro banche dati. I nomi sono altisonanti, vi figurano istituzioni e imprese italiane, come la Presidenza Consiglio dei Ministri, Roma Capitale, l'Asl di Napoli, solo per citarne solo alcuni. I dati trafugati a quanto pare, già in vendita o pubblicati su una chat di Telegram. Il rischio, secondo gli esperti di Yarix e P4I, è un enorme furto di dati.

Viviamo in un mondo in divenire, dove la maggioranza di noi sta iniziando ad orientarsi.

Ignoriamo molte delle dinamiche che si muovono in questo mondo ed alle quali siamo esposti a nostra insaputa. Vale la pena fare qualche sforzo ed adattarci il più rapidamente possibile, diventiamo consapevoli dei rischi, ma anche delle nuove possibilità che ci vengono messe a disposizione.



Bastano pochi secondi di incoscienza per trasferire in un unico colpo di mouse una montagna di dati importanti, nelle mani sbagliate.

WORM E TROJAN

Occhio al “Verme“ e al “Cavallo di Troia“

Il **Worm** è una categoria di programma malware in grado di autoreplicarsi, si diffonde rapidamente ad altri sistemi di solito grazie a connessioni di rete. Il mezzo più comune impiegato dai worm per diffondersi è la **posta elettronica**: il programma maligno ricerca indirizzi e-mail memorizzati nel computer ospite ed **invia una copia di se stesso come file allegato a tutti o parte degli indirizzi che è riuscito a raccogliere.**

I metodi con cui il Worm infetta altri computer possono essere molteplici, sfrutta vulnerabilità di basso livello nel sistema, colpendo i software presenti sul sistema facendo leva su buffer overflows, manipolazione delle stringhe, errori nella memoria e via discorrendo, in sostanza le fasi che segue il Worm per diffondersi in un sistema sono:

1. “Inietta” il suo codice nel codice di un programma benigno, come per esempio Word.
2. Manipola il codice benigno affinché questo si comporti in un modo diverso da quello originario.
3. Corrompere i dati e i file che gestisce quel programma, nel caso di Word, trasforma tutti i file DOC del sistema in Malware.

I malware non colpiscono come i virus. Nella maggior parte dei casi necessitano, di un utente distratto per infettare un dispositivo. Attenzione a dove cliccate.

Una volta che il computer del malcapitato è infettato dal Worm, quest’ultimo passa alla seconda fase del piano, ossia inviarsi ed infettare più persone possibile.

Il Trojan (prende il nome dal famoso Cavallo di Troia della guerra di Troia) è un falso file che si finge non dannoso,

come ad esempio file di documenti, fogli di calcolo, presentazioni, archivi .zip, ma una volta in esecuzione infetta il dispositivo. **Si utilizza per avere completo accesso al computer della vittima,** per poi spiare la Webcam, visualizzare file e cartelle, riprodurre audio, in pratica quasi tutto quello che si può fare al PC, l'hacker può farlo seduto comodamente da remoto.

Il Trojan **è in assoluto il Malware più pericoloso a livello di privacy** in quanto, può continuare a spiarti per mesi tramite webcam, vendere le tue immagini, i tuoi dati ed infine leggere tutto quello che scrivi… può persino ascoltare tramite microfono quello che dici.

Un Trojan è formato da 2 parti, un client ed un server, il client è quello che utilizza l'hacker per controllare il computer, mentre il server è il file che viene generato spesso dal client e deve essere inviato alla vittima, una volta cliccato da quest'ultima, l'hacker può avere pieno accesso al sistema. Una volta che il server viene eseguito, il computer della vittima genera una connessione in uscita e si collega immediatamente al client, scavalcando antivirus e firewall, dopodiché l'Hacker può fare tutto quello che vuole, mentre la vittima non ne ha nessuna idea.

Entrambe le tipologie di virus sono capaci di modificare il computer che viene infettato, in modo da essere eseguiti ogni volta che si avviano e rimangono attivi finché non si spegne o non si arresta il processo corrispondente.

COME DIFENDERSI

.01
Antivirus e scansioni

L'utilizzo di antivirus affidabili (in genere quelli affidabili non sono gratis) ed aggiornati con scansioni frequenti del sistema fanno da deterrente per possibili minacce worm e riconoscimento di file Trojan.

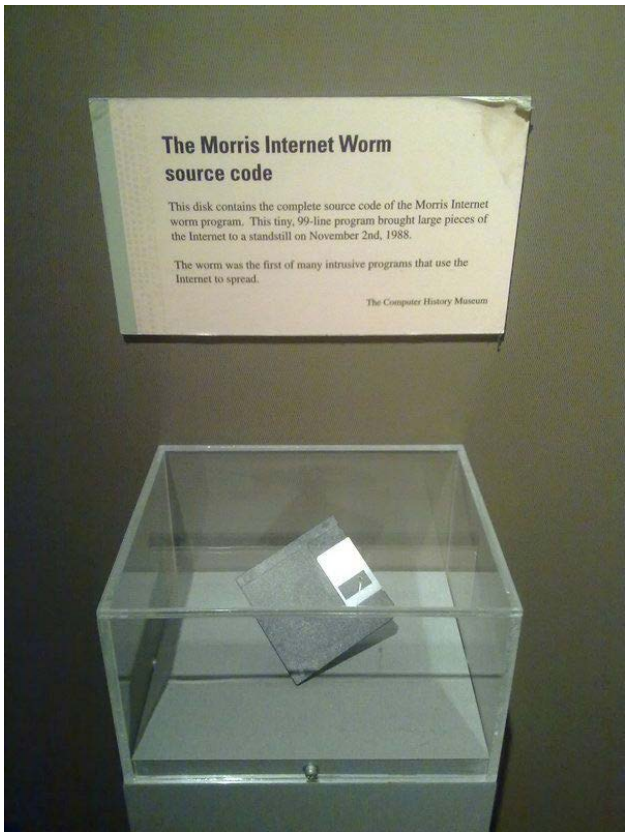
.02
Verificare sempre

Leggere attentamente l'intestazione di un'email ricevuta: accertarsi che il mittente sia verificabile, e se lo è, assicurarsi che il corpo del messaggio non presenti anomalie di scrittura o immagini e nomi dei file allegati insoliti.
È di vitale importanza comprendere questo concetto, quando si tratta di Malware niente è ciò che sembra, se ricevi una mail con dentro un documento Word o PDF, anche se conosci il mittente, prima di aprirlo, analizzalo attentamente ricorrendo all'ausilio del tuo Antivirus.

STORIA DEI VIRUS INFORMATICI

Un software che crea una copia evoluta di se stesso

La storia dei virus informatici è affascinante e risale molto più indietro negli anni di quanto crediamo. In realtà già nel 1948 John von Neumann, fisico e matematico ungherese, dimostrò matematicamente che sarebbe stato possibile creare un programma per computer che si replicasse autonomamente.
Negli anni ‘60 compare il primo programma autoreplicante, grazie ad un “gioco” creato da informatici della Bell Laboratories in cui una serie di programmi dovevano sconfiggersi a vicenda sovrascrivendosi… Giochi da nerd oserei dire!



Il termine VIRUS appare la prima volta nel 1972, nel romanzo di fantascienza “La macchina di D.I.O” scritto da David Gerrold in cui un programma informatico si comporta esattamente come i virus biologici… Il termine virus viene ampiamente usato in tutti gli anni ‘70 in romanzi film e fumetti che cominciano a “costruire” la forma che il futuro avrebbe assunto di lì a poco. E’ incredibile scoprire quanto la fantascienza sia premonitrice del nostro futuro!

Ma la consacrazione del termine e la sua definizione arriveranno solo nel 1984 ad opera della University of Southern California con Experiments with Computer Viruses dove si legge:

«Un virus informatico è un programma che ricorsivamente ed esplicitamente copia una versione possibilmente evoluta di sé stesso».

Affascinante come riusciamo a replicare gli schemi del mondo fisico e delle sue leggi anche in ambiti che apparentemente ne sono distanti.

Il primo malwere apparso al mondo è Creeper creato da Bob Thomas nel 1971 che aveva lo scopo di verificare proprio l’auto-riproducibilità di un programma su una macchina remota.

La diffusione di VIRUS per tutti gli anni ‘80 e gran parte degli anni ‘90 è stata affidata ai floppy-disk, poi con l’avvento di Internet è cambiata la modalità di trasmissione e la loro capacità di “infezione”.
La prima vera pandemia possiamo farla cadere nel 1986. Il primo virus che si guadagnò una notorietà planetaria venne creato da due fratelli pakistani proprietari di un negozio di computer, che secondo la loro versione, doveva servire a punire chi copiava illegalmente il loro software. Il virus si chiamava Brain, si diffuse in tutto il mondo.
Ma veniamo al capostipite di questa nuova generazione di virus. Era il lontano 1988, quando **Robert Morris Jr.** creò il primo worm a diffondersi via internet, il **Morris worm.** Questo gli valse anche la prima condanna legale nella storia degli Stati Uniti per pirateria informatica. Il floppy-disk che contiene il Morris worm è oggi custodito in una teca come cimelio storico al Museo della scienza di Boston.

Poi ci fù il virus **AIDS,**
la cui diffusione avveniva tramite l’inserimento di un floppy disk (è evidente l’analogia con la diffusione attraverso i rapporti sessuali), rendendo impossibile l’avvio del sistema operativo.

Nel 2000 arrivò il virus **ILOVEYOU,**
creato dall’allora studente filippino Onel De Guzman, che si propagava attraverso un messaggio di posta elettronica avente come oggetto, appunto, “ILOVEYOU”.

Il codice sorgente di questo virus è pubblicamente disponibile su Internet, e sono significative le primissime annotazioni inserite nel codice:

```
rem  barok -loveletter(vbe) <i hate go to school>
rem by: spyder  /  ispyder@mail.com  /  @ GRAMMERSoft Group  /  Manila,Philippines
```

L’autore si firma col suo nickname (“barok”), rende pubblica la sua email, dichiara la propria nazionalità oltre che il proprio odio verso la scuola (!)… in netto contrasto con l’ovvia tendenza ad eseguire questo genere di attività illegali nel più completo anonimato.

ROOTKIT E BACKDOOR

Difficili da trovare e rimuovere

Il **Rootkit** è un insieme di malware che consente di ottenere il controllo di un computer da locale o da remoto, in maniera non rilevabile dai più comuni strumenti di amministrazione e controllo.
Il termine viene da “root” che è il privilegio più alto che è possibile acquisire in un sistema, è un “kit” che consiste in programmi che aiutano l’hacker a mantenere l’accesso di root nel tempo.
I rootkit esistono da circa 20 anni, permettono agli hacker di accedere e rubare dati rimanendo nascosti nel computer anche per molto tempo. Rilevarlo può essere complicato, perchè la prima preoccupazione di questi software è bloccare i programmi che possono trovarli (antivirus).
Si può contrarre un rootkit in diversi modi, ma il più comune avviene attraverso una vulnerabilità nel sistema operativo o attraverso un’applicazione aperta sul computer. Gli hacker attaccano le vulnerabilità del sistema operativo e delle applicazioni. Usano dei codici per ottenere una posizione privilegiata sul computer della vittima. In seguito installano il rootkit e i componenti che permettono loro accesso remoto al computer. Il codice per alcune vulnerabilità può essere ospitato su siti web autentici, che sono stati compromessi. Un altro vettore di infezione è attraverso dispositivo USB. Gli hacker possono piazzare dispositivi USB con rootkit in luoghi in cui possono essere facilmente trovati dalla vittima, come uffici, caffetterie e

Contro le minacce informatiche serve pazienza e attenzione: se qualcosa sembra troppo bello per essere vero, molto probabilmente non è così bello come sembra!

congressi. In certi casi, si può contrarre un rootkit attraverso una vulnerabilità del sistema di sicurezza, mentre in altri il malware può installarsi spacciandosi per una applicazione o file apparentemente affidabile contenuto in una USB.
La rimozione può essere davvero complicata se non quasi impossibile, nei casi in cui il rootkit è riuscito ad inserirsi nella parte del sistema operativo che dialoga direttamente con l'hardware; formattare la macchina e reinstallare il sistema operativo potrebbe essere l'unica soluzione possibile.

Quando però si ha a che fare con dei rootkit nel firmware (parte hardware), la rimozione potrebbe richiedere anche la sostituzione di componenti, oppure l'utilizzo di sistemi specializzati.
Per chi crede che il sistema Windows sia l'unico che può essere colpito da un Rootkit, basti pensare che il primo è stato sviluppato per il sistema operativo Linux ed esistono anche diverse versioni per MacOsx.

Al rootkit si abbina la **Backdoor** che è un programma indipendente (riesce ad essere eseguito in autonomia) ed ha due componenti: il Server e il Remote. Il server è installato nel sistema vittima e il remote è lo strumento per controllare da remoto il sistema della vittima.
Il server cerca di nascondersi nei file di sistema assumendo nomi e dimensioni che non diano nell'occhio, così da non mettere in allarme il programma Antivirus né tanto meno un utente. Basta un comando in remoto da parte del cybercriminale per trasformare questo file all'apparenza innocuo in una via di accesso privilegiata al sistema. Una volta attivate, permettono praticamente qualunque operazione: dal controllo su tutti i processi attivi, compreso la gestione di webcam, mouse e tastiera.

COME DIFENDERSI

.01
Aggiornamenti sempre
Mantieni aggiornato il sistema operativo

.02
Antivirus
Installa un buon Antivirus, sempre a pagamento, e mantienilo aggiornato

.03
HTTPS
Non inserire MAI i tuoi dati personali su siti che non utilizzano il protocollo di trasmissione dei dati HTTPS (con la S finale)!

.04
Attenti al sito
Non visitare siti web non attendibili, come siti di pornografia, pirateria informatica e categorie simili.

.05
Software sicuri
Fai attenzione a cosa installi. Investi in software sicuri, conosciuti e a pagamento, da cui sai con certezza che non corri rischi.

.06
Firewall
Utilizza il firewall (consigliato di tipo hardware). I firewall aggiungono un livello di protezione in più al sistema informatico, obbligando i malware a trovare altri percorsi in entrata e in uscita.

.07
Controlla i download
Attenzione ai download. I rootkit sono tanto insidiosi da essere in grado di nascondersi anche nei file di PDF. A volte basta scaricarne uno e alla prima apertura del PDF il rootkit si installerà sul tuo computer.

.08
Buon senso
Buon senso, buon senso e per finire buon senso! Prenditi sempre qualche secondo per valutare l'attendibilità delle pagine su cui navighi. A volte rinunciare alla soddisfazione istantanea di scaricare ciò che cerchiamo da Internet può risparmiarci molti problemi.

PHISHING E SPAM

Come un pesce preso all'amo nel mare delle mail

Il phishing è una delle minacce informatiche più conosciute, ma allo stesso tempo una di quelle in cui continuiamo a cascare troppo spesso. È una truffa telematica che ha l'obiettivo di carpire le informazioni ed i vostri dati personali. Deriva dal termine "andare a pescare", ed è proprio quello che fanno gli hacker quando adottano questa tecnica.

In pratica, un malintenzionato cerca, attraverso una mail, di ingannare la vittima convincendola a fornire informazioni personali, dati finanziari o codici di accesso riservati, fingendosi un ente affidabile, una banca, un ente governativo ecc.

Si concretizza in una mail contraffatta in cui si invita il destinatario a fornire dati riservati, motivando tale richiesta con ragioni di ordine tecnico o conferma dati. Può capitare che il messaggio sembri provenire proprio dalla nostra banca, un attimo di panico, un momento di superficialità e il gioco è fatto, siamo finiti allamati come un povero branzino.

Per la maggior parte è una truffa perpetrata usando messaggi di posta elettronica, ma non mancano casi simili che sfruttano altri mezzi, quali i messaggi SMS, su social o chat quali, Whatsapp, Instagram, Telegram ecc...

Il canale usato in genere sono gli spam, sono messaggi indesiderati, inviati in maniera automatica e massiva. Possono anche avere scopi malevoli oltre alla frode informatica.

Esiste una metodologia di phishing estremamente pericolosa chiamata **SpearFishing**. In pratica a differenza del phishing classico, dove il phisher invia una quantità elevata di email aspettando che qualcuno caschi nella sua trappola, nello Spear Phishing viene inviata una email ad una specifica persona od organizzazione che si è studiata approfonditamente in precedenza. In pratica il phisher studia la vittima e prepara un attacco specifico che naturalmente ha una percentuale di successo più elevata rispetto al phishing classico. A differenza delle email di phishing nelle quali la comunicazione è generalmente impersonale, in questo caso si viene chiamati per nome, vengono fatti riferimenti precisi, ad esempio, si fa cenno ad un superiore che ha richiesto di compiere delle operazioni. Proprio per la conoscenza che il phisher ha di noi si tratta di azioni particolarmente efficaci che necessitano di attenzioni che possono essere assunte con l'utilizzo di semplici protocolli o abitudini di sicurezza.

Purtroppo la reale tutela nel mondo virtuale avviene soprattutto adottando comportamenti consapevoli che ci eviteranno di cadere nei tranelli ai quali questa nuova dimensione ci sottopone ogni giorno.

Il Phishing o lo SpearFishing sono a tutti gli effetti una forma di adescamento: l'hacker inganna l'utente, sfruttando le sue paure, per carpire informazioni come login e password per accedere alla sua banca on line o documenti di identità e codice fiscale che poi possono essere utilizzati per compiere una serie di azioni illegali, senza che l'interessato ne venga a conoscenza… almeno fino alla resa dei conti.
Ad esempio, il criminale potrebbe avere l'opportunità di usare il tuo nome e cognome per vendere online della

merce inesistente: farsi pagare e poi scomparire, lasciando che siano a vostro carico sia le denunce che il processo per truffa.
Oppure, immagina che un “amico” ti invii un messaggio o una mail con un link simile a questi di seguito. Di solito si chiede di controllare o verificare dati o guardare una foto o leggere un testo. Il tutto per indurti a eseguire il clic.

https://www.facebook.com+settings&tab=privacy@%3192%2E%3168%2E%31%2E%38

http://google.com@accounts@%3192%2E%3168%2E%31%2E%38

https://www.facebook.com+settings&tab=privacy@0300.0250.0001.0010

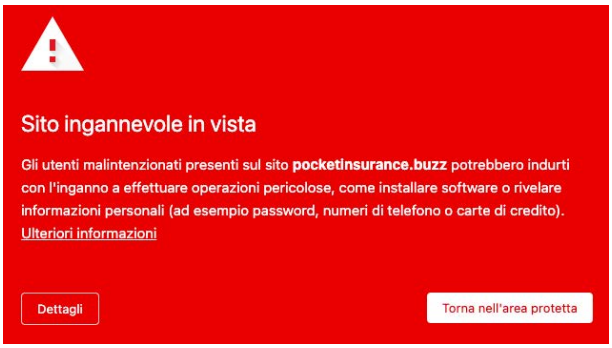
Non abboccare !
Seguendo il link, andrai su un server che ha indirizzo IP 192.168.1.8 o simile, dove troverai un clone della pagina di autenticazione di Facebook o Google… oppure della tua banca. Una volta digitate le tue credenziali le avrai consegnate al tuo “amico”. Per rendere la truffa perfetta verrai re-indirizzato sul vero sito, in modo che non ti accorga neanche di aver consegnato i tuoi dati. Dal quel momento il tuo “amico” avrà pieno accesso alla tua vita!

Molto spesso gli utenti non sono in grado di riconoscere una email di PHISHING e vi cadono facilmente vittima, mettendo in pericolo la sicurezza dei dati aziendali.

Purtroppo di solito, non sono gli amici che fanno questi giochetti, ma hacker che utilizzano una mail, o un SMS di una persona che conosci per aggirare le Tue difese.

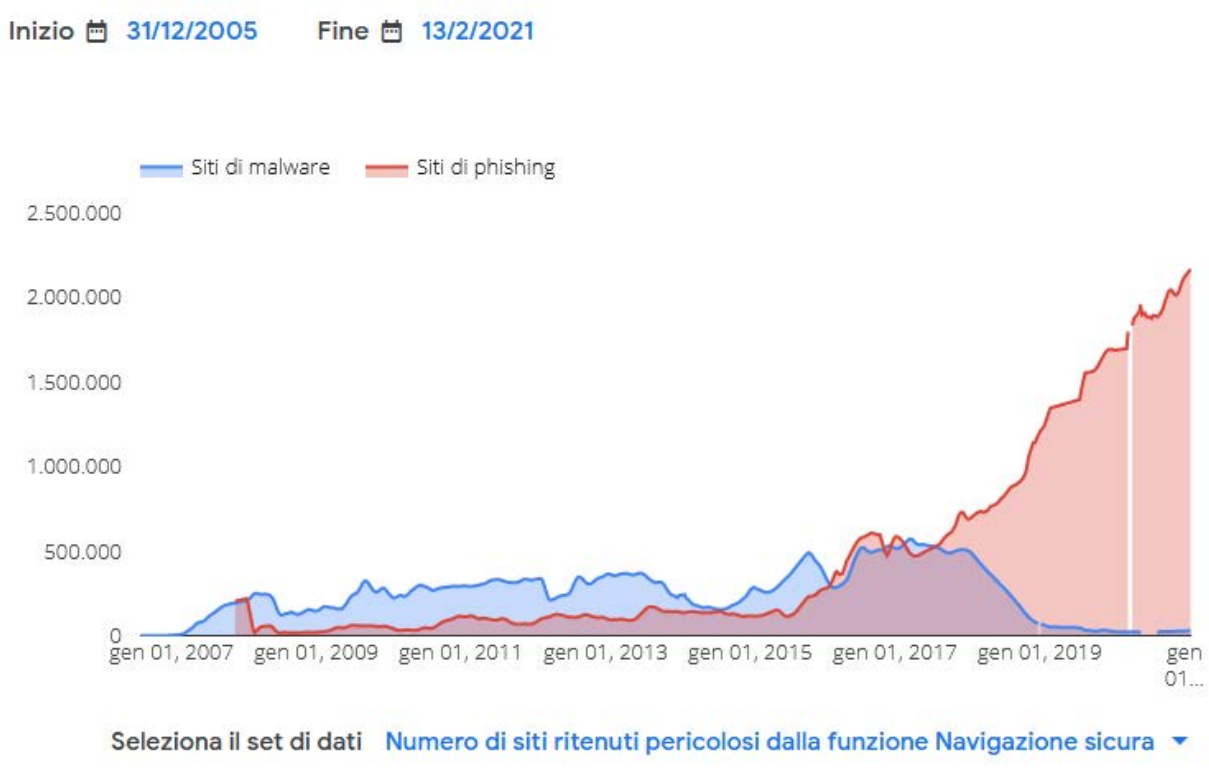
L’anno 2020 ha visto un aumento notevole delle e-mail di phishing, molte sono state quelle che hanno sfruttato il tema “Covid”, e lo “smart working”, queste hanno fatto uso principalmente di due metodi di contagio: il primo con il classico documento allegato contenente malware e il secondo con collegamenti ipertestuali verso siti malevoli.

Nella top-ten mondiale di e-mail a tema Covid-19 con allegato, c'è stata una mail circolata in Italia con oggetto: "Coronavirus – Informazioni importanti su precauzioni", questa e-mail aveva come falso mittente l'Organizzazione Mondiale della Sanità e invitava a cliccare su un file Word contenente le informazioni sulle precauzioni da prendere per evitare contagi.



Questa e-mail è risultata molto "aggressiva" nella prima fase della pandemia, perché tutti in quella fase eravamo alla ricerca quasi spasmodica di informazioni su quali potessero essere i giusti comportamenti da adottare. Nella primavera del 2020 si è evidenziata con estrema chiarezza la crescita impressionante del numero di siti Phishing.

Google Navigazione Sicura
(servizio per la sicurezza che Google ha sviluppato per identificare i siti non sicuri e informare utenti e webmaster del potenziale pericolo) in un report ha censito un crescita esponenziale da circa 30.000 siti Phishing individuati, a circa 188.000 nel momento peggiore, per poi attestarsi a oltre 40.000 alla fine del periodo di picco pandemico.



COME DIFENDERSI

.01
Essere diffidenti
Anche se il mittente della email potrebbe sembrare attendibile non è detto che lo sia.
Non scaricare mai allegati anche semplicemente file word, perché potrebbero contenere malware. Chiedetevi sempre se la email ricevuta ha un senso, se conoscete il mittente, se ha qualcosa di strano come destinatari multipli a voi sconosciuti.

.02
Controlla i link
A questo indirizzo potete controllare i link sospetti:

https://transparencyreport.google.com/safe-browsing/search

.03
...chi ti conosce
Passando con il mouse sopra eventuali link controllate che il sito di destinazione sia effettivamente quello fidato.
Diffidate di email provenienti da enti governativi che vi richiedono di scaricare i file allegati.

.04
Come parli bene...
Occhio alle email sgrammaticate, o che presentano errori ortografici, molto spesso sono state fatte da traduttori automatici. Sono uno dei segni caratteristici di questo tipo di minaccia.

.05
Io non pago!
Non pagare riscatti in criptovaluta a fantomatici personaggi che dicono di avere vostre informazioni compromettenti.

NotPetya killer per la Cyberwar

Il 27 giugno 2017, a Copenhagen, il gruppo A.P. Møller-Maersk, che opera in tutto il mondo, con 574 uffici, in 130 Paesi, rischia di collassare completamente. Responsabile di un quinto delle operazioni mercantili su nave – con 76 aree portuali controllate e quasi 800 imbarcazioni – l'infrastruttura tecnologica che la sostiene all'improvviso "non funziona" più.
Il 27 giugno, tutti gli schermi dei computer degli impiegati della sede danese cominciano a diventare neri. Su alcuni compare la scritta "repairing file system on C:", su altri "oops, i tuoi file importanti sono criptati", chiedendo in cambio il valore corrispondente a 300 dollari in bitcoin per decrittarli.

Nel giro di 30 minuti, alcuni impiegati della multinazionale cominciano a correre per gli uffici, gridando a tutti di spegnere o disconnettere tutti i computer, prima che sia troppo tardi. In circa due ore, Maersk riesce a disconnettere completamente il proprio network globale, bloccando del tutto le operazioni nei numerosi porti controllati.
Il danno ai server è però ormai compiuto: i dirigenti del gruppo mandano a casa anche i dipendenti del reparto IT, perché non c'è più nulla da fare.
Solo per un caso fortuito, Maersk riuscirà poi a recuperare tutti i propri dati. Ad alcuni giorni dall'attacco, gli esperti dell'azienda e centinaia di consulenti Deloitte arruolati allo scopo, riescono a venirne a capo. Sono occorsi due mesi per rimettere in piedi tutto il processo e l'attacco è costato a Maersk tra i 250 e i 300 milioni di dollari.

Pandemia Sanitaria e Informatica

Secondo il Security Summit Streaming Edition, la maggioranza degli attacchi (61%) legati al coronavirus riguarda campagne di phishing, cioè truffe informatiche via email, in associazione a malware (21%), ossia software dannosi. Il 64% degli attacchi è strutturata per danneggiare rapidamente e in parallelo il maggior numero di persone ed organizzazioni. L'11% è legato al mondo sanitario e il 12% a bersagli governativi, con attacchi per approfittare, nelle prime fasi concitate di approvvigionamento di presidi di sicurezza, ad esempio le mascherine, creando danni considerevoli.

Unicredit: banca dati violata nel 2015

In Italia la banca Unicredit ha denunciato un po di tempo fa la violazione dei dati di 3 milioni di suoi clienti avvenuta pare nel 2015. Cosa significa? Significa che un cyberattacco costa molto denaro e non può essere nascosto per sempre. Le violazioni dei dati possono costare alle aziende milioni di danni.

RANSOMWARE E CRYPTOLOCKER

Bloccare file e sistemi in cambio di soldi

Il ransom malware, o **ransomware**, è un tipo di malware tra i più pericolosi. Blocca l'accesso ai sistemi o ai file personali degli utenti al fine di ricevere il pagamento di un riscatto per renderli nuovamente accessibili.

In genere il Ransomware viene unito ad un Worm per essere diffuso, in modo che possa colpire più persone possibile, replicarsi e auto inviarsi a tutti i contatti della email o social network. Quando infetta il computer non si presenta subito, infatti prima scannerizza le directory del nostro pc, cripta dei file e solo dopo aver compiuto tutti i passaggi, si manifesta e chiede il riscatto.

I ransomware sono:

lock screen (blocco immagine) che sfruttano un'immagine a schermo intero o una pagina web per impedire l'accesso al computer;
encryption (crittazione) che bloccano i documenti presenti nel computer criptandoli con una password e rendendo impossibile aprire i file.

Il **criptolocker** è una forma di ransomware della categoria encryption, specifico per sistemi Windows, che critta i dati della vittima e richiedere un pagamento per la decrittazione.

Questa tipologia di virus viene diffusa principalmente attraverso le email, adescando chi facilmente si fa distrarre da email contraffatte. Dopo aver cliccato sul documento allegato, il malcapitato, installerà inconsapevolmente il malware che inizia a crittare i dati.

Di solito rinomina i file, aggiungendo al nome file, una serie di lettere e numeri rendendoli inutilizzabili. Nel tentativo di accedervi apparirà il messaggio che riporta la richiesta di riscatto… Pensa che terribile esperienza! da soli davanti al proprio computer ostaggio di chissà chi senza poter fare nulla.

Talvolta alcune aziende sottovalutano le conseguenze di un attacco ai propri sistemi informatici. Oggi, la possibilità di comunicare con fornitori, clienti, dipendenti e reparti attraverso gli strumenti telematici, oltre alla gestione e conservazione documentale (che include, talvolta, anche importanti documenti aziendali), è d'importanza strategica e un "blocco" forzato della Rete può avere dei costi molto alti, anche in termini reputazionali (es. non riuscendo a rispettare le scadenze).

La sicurezza informatica riveste ormai un ruolo prioritario in ogni azienda, istituzione, impresa che abbia anche solo un PC al suo interno. E anche per ogni famiglia e ogni singola persona che possegga uno smartphone, spesso ignara delle conseguenze che un attacco può avere a un sistema "casalingo" (immaginate semplicemente che qualcuno entri in possesso del vostro PC o del vostro smartphone).

COME DIFENDERSI

.01
Siate consapevoli
La miglior protezione è la prevenzione. Il primo passo da fare è aggiornare sempre sia il nostro antivirus che il sistema operativo.

.02
Ogni giorno è un buon giorno per fare il Backup dei Dati
Fare sempre un backup dei dati, cioè una copia dei propri file, è importante che il backup venga eseguito spesso ed in modo completo in un hard disk esterno. In questo modo, se il ransomware dovesse infettare il pc, una copia dei dati rimarrebbe protetta, dandoci l'opportunità di ripristinarli.

.03
Utilizzare Firewall di rete
Assicurarsi che tutto il traffico sia sottoposto a controllo tramite firewall questo consentirà a molte delle protezioni di applicarsi a tutto il traffico generato in entrata ed uscita.

.04
Utilizzo di utenti non amministratori
Utilizzare – quando possibile – account senza diritti da amministratore: un utente non-amministratore ha privilegi limitati e le stesse limitazioni si trasferiranno in mano all'attaccante.

.05
Naviga con una VPN
Per i collaboratori in SmartWorking far utilizzare sempre una rete privata virtuale (VPN-Virtual Private Network)

.06
Fare formazione
Addestrare i dipendenti su come riconoscere le minacce e su come segnalare in modo veloce eventuali incidenti di sicurezza sospetti.

.07
Assicuratevi di avere un piano di disaster recovery
Un piano di disaster recovery e business continuity che preveda il recupero a seguito di attacco da ransomware.

ATTACCO DDOS

Un lavoro per i corpi speciali

Un attacco **DoS** (Denial of Service) si propone di impedire l'uso di una risorsa di rete, ad esempio un sito web. Quando all'attacco partecipano molti sistemi, spesso dell'ordine di decine di migliaia, si parla di **DDoS** (Distributed DoS) ed è facile capire perché sia molto più devastante e difficile da bloccare.

Un attacco di questo tipo è un metodo che gli hacker utilizzano per impedire o negare agli utenti legittimi l'accesso a un computer. Gli attacchi sono eseguiti con strumenti che inviano ripetutamente decine, centinaia o migliaia di richiesta a un server Internet (Web, FTP, di posta), impegnando tutte le risorse del server, al fine di renderlo inutilizzabile.

Una minaccia informatica tanto semplice da mettere in pratica, quanto efficace: capace di mandare in tilt un'azienda, o infrastrutture aziendali strategiche. Consiste nel tempestare di richieste un sito, fino a metterlo KO e renderlo irraggiungibile. Stando agli ultimi dati dell'associazione italiana per la sicurezza informatica, **è tra gli attacchi che colpiscono un'impresa ogni cinque minuti insieme ai malware e ai ransomware.** Difendersi è molto difficile ed è meglio attrezzarsi prima.

L'autore di questo tipo di attacco, può anche richiedere un pagamento per interrompere l'attacco. Attacchi DDoS sono utilizzati per distrarre l'attenzione da altre attività criminali simultanee, ad esempio truffe bancarie, oppure contro istituzioni governative o finanziare, o anche contro siti di e-commerce per motivi di concorrenza.
Si possono distinguere tre tipologie: **attacchi volumetrici,** che cercano di saturare la banda della vittima, **attacchi di protocollo,** che consumano le risorse del server **e attacchi a livello applicativo**, ad esempio saturando di richieste un server web. Spesso i tre tipi sono mescolati.

COME DIFENDERSI

.01
Prevenzione
Una possibile contromossa rispetto a questo tipo di attacchi è la progettazione e la creazione di infrastrutture scalabile e resiliente fin dall'inizio (database, firewall, e così via).
L'utilizzo di Regole Firewall che impediscano e blocchino i tentativi di accesso ai sistemi da Indirizzi IP remoti sconosciuti.

.02
Password
Effettuare il cambio password periodico elaborando password di almeno 8 caratteri compresi Maiuscole, minuscole, numeri e caratteri speciali.

Luxottica: un esempio di difesa efficace

Nel settembre del 2020 un attacco ransomware causa il blocco totale delle attività produttive di Luxottica, la più grande azienda di occhiali al mondo con oltre 80.000 dipendenti e 9,4 miliardi di fatturato nel 2019.
Dunque, quello che inizialmente era stato descritto dalla stessa azienda come un "guasto al sistema informatico" che ha causato la sospensione del secondo turno produttivo negli stabilimenti di Agordo e Sedico, nel bellunese, e il blocco delle attività produttive in Cina, sarebbe stato in realtà un vero e proprio "tentativo mosso dall'esterno di entrare negli apparati informatici Luxottica". A confermarlo, una nota del sindacato Femca-Cisl.
La buona notizia è che la chiusura preventiva degli apparati informatici e la corretta configurazione dei sistemi di difesa del colosso dell'occhialeria pare abbiano consentito di respingere l'attacco dei criminal hacker impedendo l'accesso e la conseguente sottrazione di dati e informazioni riservati su utenti, consumatori e proprietà intellettuali dell'azienda.
Il malware, prontamente individuato e isolato, non avrebbe quindi causato alcun danno all'infrastruttura, mentre è stata rapidamente completata l'opera di bonifica della rete di server interessati dall'attacco informatico. Alla fine non c'è stato alcun data breach, mentre l'attività produttiva sta pian piano tornando alla normalità.

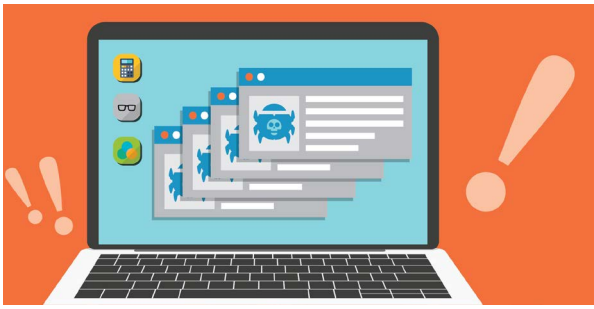
L'attacco ransomware subito da Luxottica deve dunque servire da lezione per tutte le aziende e le organizzazioni pubbliche e private.
Dal Checco (esperto di informatica forense) ci fa notare che "i tempi sono cambiati, devono quindi cambiare anche le contromisure, sempre più difficili da attuare, soprattutto perché una volta compromesso il sistema e prelevati i dati, c'è poco da fare".
"Se non si hanno copie di sicurezza da qualche parte", é stata la considerazione finale del nostro esperto, "i dati molto raramente si recuperano: i criminali saranno anche "cattivi" ma non sono ingenui, hanno ormai imparato come non lasciare tracce, come cifrare in modo corretto, silenzioso, permanente, a modo loro efficace".
In questo senso, anche l'analisi di quanto successo lo scorso anno durante l'attacco ransomware all'italiana Bonfiglioli Riduttori può essere lo spunto giusto per ricordare a tutti, ancora una volta, quanto importante sia la security awareness aziendale. I tempi sono maturi, ormai, affinché tutte le aziende comprendano finalmente che anche la sicurezza informatica delle proprie infrastrutture e dei dati deve diventare un asset strategico per la crescita e lo sviluppo competitivo delle aziende stesse.

Fonte: cybersecurity360.it

ADWARE E JOKE

Pubblicità e comportamenti del browser inaspettati

L'Adware è un programma sponsorizzato da pubblicità che raccoglie segretamente informazioni personali e le invia a un altro computer, in genere per scopi pubblicitari. Non pensare che si tratti di poca cosa, da alcuni dei nostri dati si possono estrarre informazioni molto preziose per un malintenzionato, e poi diciamocela tutta: a chi fa piacere diventare una merce ed essere venduto a chissà chi?
Questo tipo di programmi tengono traccia di informazioni sull'utilizzo del browser Internet o di altre abitudini dell'utente.
Gli Adware possono presentarsi in varie forme, attraverso le classiche toolbar indesiderate, la comparsa di pubblicità su siti che visitiamo giornalmente, la disattivazione di plug-in del browser che bloccano la pubblicità e la manomissione dei risultati di Google, inoltre quando abbiamo un Adware installato sul nostro computer, permettiamo all'hacker di mostrarci qualsiasi tipo di advertising pubblicitario, può farci cliccare, scaricare o visualizzare qualsiasi tipo di contenuto e se riesce ad infettare molte persone, può iniziare a guadagnare cifre non indifferenti.



JOKE è un programma che modifica o interrompe il normale comportamento del computer creando un fattore di distrazione o fastidio all'utente.
L'attacco, in genere, avviene durante la navigazione online con il browser fidato, a un certo punto si assiste all'assalto di finestre pubblicitarie che compaiono all'improvviso, scorrono dai lati della schermata o spuntano in altro modo interrompendo e re-indirizzando l'attività. Nonostante i tentativi di chiusura, le finestre continuano a comparire. Una volta conquistato il dispositivo, l'adware può svolgere tutta una serie di attività indesiderate. Alcune delle funzionalità sono progettate per analizzare le posizioni e i siti internet visitati, per poi presentare pubblicità pertinente ai prodotti e ai servizi collegati.

COME DIFENDERSI

.01
Attenzione ai Siti
Evitare di scaricare programmi, anche se gratuiti, da siti internet non ufficiali e potenzialmente rischiosi.

.02
Aggiornamenti da Siti Ufficiali
Mantenete aggiornati sistemi operativi e antivirus.
Non cliccate su pop-up che richiedono di aggiornare programmi e sistema operativo (in caso di dubbi, rivolgetevi al produttore).

.03
Vi servono quelle estensioni?
Fate attenzione, alle estensioni installate nei browser.

.04
Allegati Pericolosi
Non aprite, link e allegati email sospetti.

HIJACKER

Attenzione "Dirottatore" a bordo

Sono programmi che genericamente vengono richiamati da controlli Active-X. Una volta aggredito il computer, si amalgamano al browser di navigazione web cambiando i parametri di protezione e le impostazioni di default.

Molti programmi di dirottamento del browser sono inclusi in pacchetti di software che l'utente non ha scelto e vengono erogati in maniera quasi occulta.

Durante le procedure di installazione di molti programmi gratuiti si nascondono queste minacce, e sono il luogo dove potremmo intervenire per evitarle. Non è sempre facile trovare il modo per evitare di installarli.

Spesso, questi componenti, si presentano privi di istruzioni di disinstallazione o documentazione su ciò che fanno e sono progettati per essere fonte di confusione per l'utente medio.

COME DIFENDERSI

.01
Attenzione
Fai molta attenzione durante l'installazione di nuovi software. Evita programmi, app e siti web sospetti o poco conosciuti.

.02
Leggi Feedback
Non installare plugin non verificati e poco conosciuti. Leggi i commenti e i feedback degli utenti prima di installarli.

.03
Sempre Antivirus
Installa un antivirus potente e possibilmente a pagamento e tienilo sempre aggiornato

.04
Aggiornamenti
Mantieni aggiornato il sistema operativo. Se utilizzi Windows, passa all'ultima versione, che impedisce la modifica automatica delle impostazioni di navigazione e del browser.
Imposta gli aggiornamenti automatici.

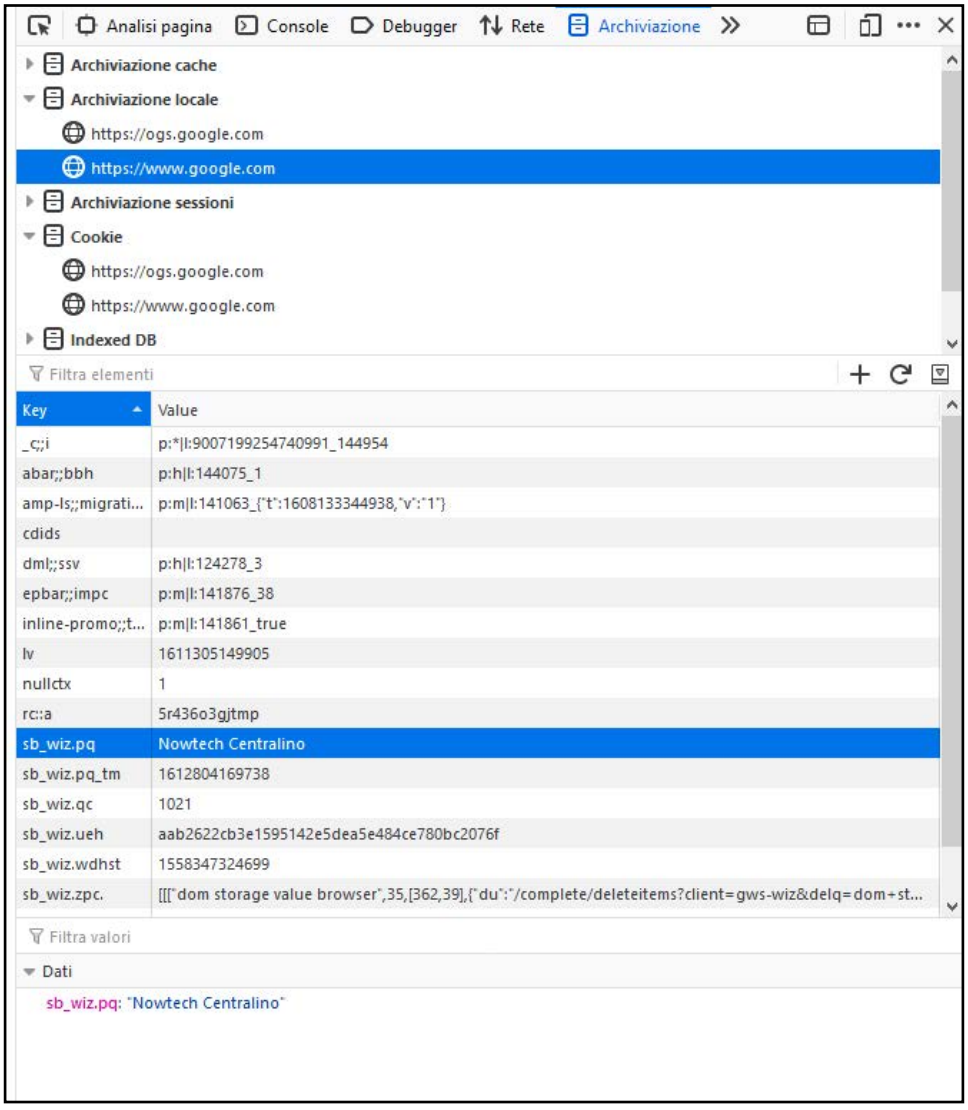
COOKIE
E DOM STORAGE

Partiamo dalla semplice definizione. I cookie sono un tipo particolare di file (una sorta di gettone identificativo) e vengono utilizzati dalle applicazioni web per archiviare e recuperare informazioni sui computer ed utenti che navigano sul sito web.

In pratica sono dei file scritti nel nostro HardDisk che vengono creati da un sito web quando vi accediamo. Questi cookie possono contenere informazioni di qualsiasi genere, come login a siti web (es gmail, youtube ecc…) ma anche informazioni pubblicitarie.
Vi è mai capitato di fare una ricerca per un articolo da acquistare, e dopo poco, visitando altre pagine, vi trovate annunci pubblicitari di offerte relativi a prodotti dello stesso genere?
Ebbene questo è colpa dei cookie.
I cookie, hanno diverse funzioni, tra quelle che maggiormente mettono a rischio la nostra privacy sono quelle che tracciano la nostra navigazione, infatti l'NSA (l'organismo del Dipartimento della difesa degli Stati Uniti d'America che si occupa della sicurezza nazionale) li utilizza per tracciare le attività online dei soggetti da monitorare. Questi sono anche pericolosi poiché essendo salvati nel nostro HardDisk sono accessibili anche da altri programmi, che potrebbero utilizzarli per carpire informazioni personali importanti come password o email. Fermare la piaga dei cookie ed Impedire completamente ai cookie di essere salvati nel nostro disco è possibile ma

sconsigliato poiché alcune pagine web potrebbero non funzionare correttamente o addirittura bloccare la navigazione.
Ma allora come facciamo a limitare i danni? Il metodo più semplice da mettere in pratica è la modalità in incognito. Una modalità di navigazione disponibile su tutti i browser.

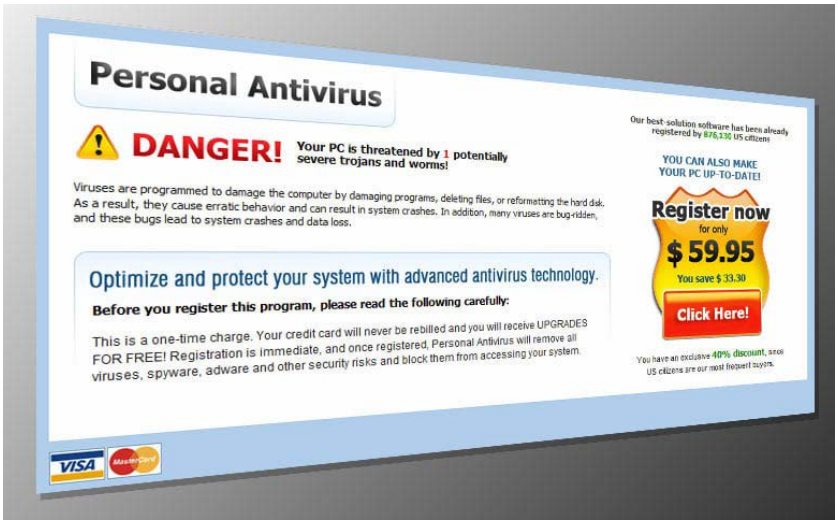
DOM Storage
Sono i dati salvati dal browser per consentire il veloce recupero di pagine web visitate in precedenza e per velocizzare la navigazione.
I dati DOM Storage non hanno l'impostazione della scadenza e possono essere permanenti, a differenza dei cookie. Il controllo è lasciato in mano agli utenti.
Per disattivare il DOM Storage andiamo nella pagina dedicata alle impostazioni del browser ed annulliamo tutti i permessi di memorizzazione.



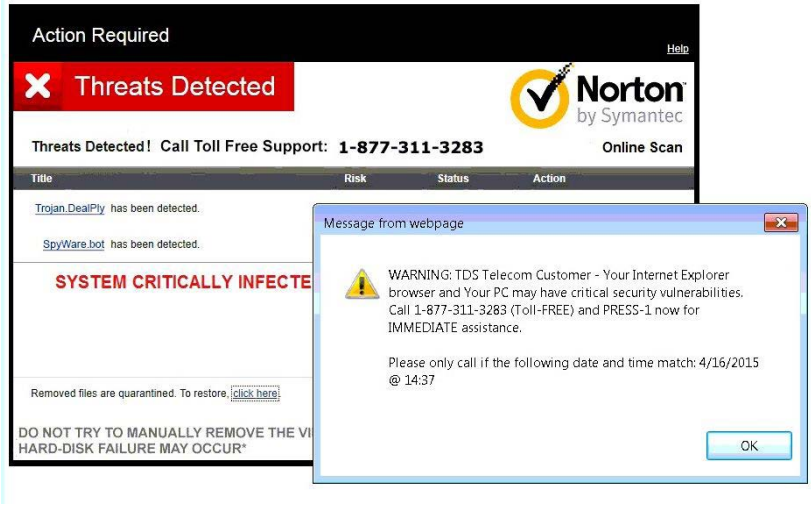
SCAREWARE

Sono dei programmi inutili e dannosi che vengono installati dall'utente quasi inconsapevolmente e che preparano la strada agli hacker per intentare una truffa.
I pirati informatici, oltre a studiare nuove tecniche di hackeraggio, hanno cominciato a leggere anche i libri di marketing. E gli scareware ne sono la dimostrazione.
Per convincere gli utenti a installare questo tipo di software utilizzano le stesse tecniche dei pubblicitari.

Mostrano sul computer messaggi del tipo
"ATTENZIONE! Il tuo computer è stato infettato.
Scarica questo programma per eliminare il virus".
Una persona poco attenta alla sicurezza informatica può tranquillamente cadere nel tranello architettato dagli hacker. E installare sul proprio computer uno scareware.
Quando si scarica un software da Internet, non sempre si tratta d programmi "buoni". E gli scareware fanno parte del gruppo "software cattivi". Si tratta di programmi che non sono dei veri e propri virus, ma che sono praticamente inutili sul PC. Se li installiamo non risolvono nessuno dei problemi che segnalano. Anzi, li amplificano.



Solitamente il messaggio appare sotto forma di pop-up mentre si sta navigando su Internet.



Se si scarica e si installa il programma sul PC, partirà una finta scansione antivirus che porterà al ritrovamento di malware e spyware che stanno infestando l'hard disk. Per rimuoverli, lo scareware suggerisce all'utente di acquistare la versione definitiva del programma. Logicamente la scansione antivirus è fasulla e sul PC non è presente nessun virus. Se per la paura si acquista il programma, non solo si rivelerà un software inutile ma si inviano i dati della carta di credito a un hacker. Oltre alla truffa anche la beffa.

Gli scareware si incontrano soprattutto mentre si naviga su Internet con il computer, ma ormai è frequente incontrarli anche sullo smartphone. Se mentre stiamo giocando a qualche applicazione, appare una pubblicità che sponsorizza un'app che ottimizzerà il device cancellando foto e video inutili, non dategli retta, si tratta di uno scareware.
In alcuni casi gli scareware nascondono anche dei veri e propri virus. Quando si andrà a installare il software inutile si aprirà la porta a virus, spyware e malware.

COME DIFENDERSI

.01
Buon senso
Quando vi si presenta un messaggio che vi invita a installare un programma per eliminare i virus, chiudete la finestra e continuate a navigare tranquillamente su Internet.

.02
Antivirus affidabili
installate sempre antivirus affidabili, nella maggior parte dei casi i programmi di sicurezza sponsorizzati dagli scareware sono sconosciuti ed inaffidabili.

IL CLOUD

In inglese significa nuvola, si pronuncia “Clàud“

“Cloud” è un termine inglese che significa “nuvola”, quindi è una “nuvola” di dati e servizi sempre accessibile da una connessione internet, da qualsiasi dispositivo ed in qualsiasi luogo.

Se ben gestito è una grande evoluzione tecnologica offerta dalla rete.

Quando si dice salvare i tuoi dati nel cloud, si intende semplicemente salvare i tuoi dati in servers accessibili tramite connessione Internet, dal tuo computer o dal tuo cellulare, ovunque ti trovi.

Anche senza saperlo, con tutta probabilità usi quotidianamente il cloud quando navighi ed usi Internet, per la posta, le foto, la musica o per i giochi.

Il “cloud” è una rivoluzione – tuttora in corso – nel mondo di Internet, sia per le persone che per le aziende. Grazie al cloud, chiunque può accedere a programmi e servizi tramite Internet che altrimenti richiederebbero ingenti risorse economiche per funzionare. Questo è il cosiddetto “cloud computing”: utilizzo di **applicazioni e servizi tramite internet.**

Un’azienda potrebbe ad esempio aver bisogno di un programma Gestionale oppure di un CRM.

Prima del cloud l’azienda avrebbe dovuto acquistare la costosa licenza per l’utilizzo del software, mettere in piedi un team di esperti hardware e software per installare, con-

figurare, testare, eseguire, proteggere e aggiornare il programma acquistato. Oggi invece, grazie al “cloud computing”, le aziende “affittano” i servizi via cloud o pagano in base al consumo, sempre comunque accedendo tramite cloud al servizio.
Il fornitore del servizio cloud, chiamato “hosting service provider“, gestisce tutto ciò che riguarda hardware e software al posto dell’azienda.
Gli aggiornamenti sono automatici, e i dati sono duplicati in più data centers (edifici dove sono ospitati centinaia o migliaia di servers) per garantire sempre l’integrità e la disponibilità dei dati all’utente.
Anche in caso di guasti tecnici o attacchi di hackers ai servers di un data center, l’hosting provider può recuperare e duplicare nuovamente i dati. Quindi non c’è il rischio di perderli poichè vengono duplicati più volte in più sedi geografiche diverse.
Il cloud è comodo. Permette di rendere versatile il nostro lavoro perché vuol dire avere i nostri dati a portata di mano ovunque siamo. Potremmo chiamare il Cloud: “ufficio virtuale”, ognuno affitta una o più stanze proprie per i suoi contenuti, gli spazi comuni sono visitabili da chiunque, mentre le stanze private potenzialmente non lo sono.
Certamente chi ha la chiave d’accesso alla nostra stanza può entrare facilmente e prendere tutto ciò che vuole.

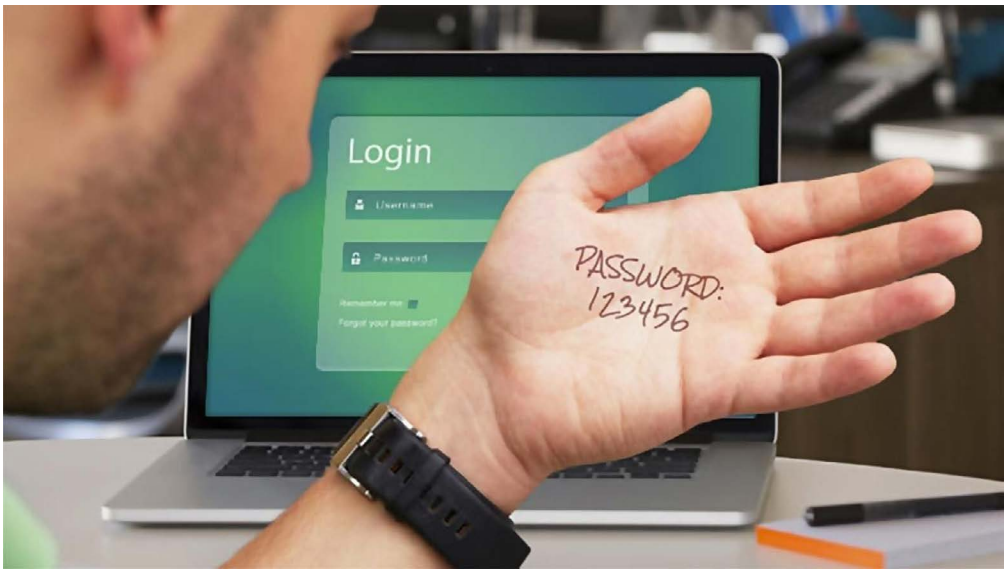
Le chiavi in questo mondo si chiamano Credenziali o Account e sono composte da nome utente e password.
Viene da sé che gli Account sono tra le cose più importante da proteggere. Purtroppo spesso ciò che ci identifica sulla rete non viene trattato con la giusta riservatezza, viene per esempio lasciato su di un foglio di carta appeso al Computer. Capita più spesso di quanto si possa immaginare che si lasci la propria postazione senza mettere il computer in sicurezza, aggiungendo uno stop ed una password per la riattivazione; così facendo chiunque può prendere il controllo della macchina ed estrarre tutti i dati custoditi.

Chi ha le nostre chiavi di accesso controlla le nostre azioni!

SICUREZZA DELLA PASSWORD

Fare password efficaci in modo semplice

Sembra impossibile che un hacker possa entrare in possesso delle nostre password. Quando questo succede accogliamo l'avvenimento con sorpresa, stupore... come è potuto succedere?
La risposta a questa domanda è complessa ma cerchiamo insieme di fare un po' di chiarezza su questo argomento fondamentale della sicurezza informatica. Le possibili cause sono legate principalmente a due scenari differenti:



La password utilizzata è "debole"
Per "debole" si intende che la utilizzate su tutti i vostri siti (avete una sola password o pochissime che cambiate troppo raramente) Una password si definisce debole se con attacchi a **forza bruta** o a **vocabolario** è possibile identificarla in un tempo ristretto. Significa che un Hacker con strumenti automatici di generazione password è in grado di trovarla in un tempo brevissimo.

Una password è debole quando è corta
Contiene solo lettere o caratteri, contiene i vostri nomi o dei vostri parenti oppure le parole del vocabolario.
Ogni anno un'azienda della silicon valley pubblica la lista di quelle più utilizzate in base a dei campioni di password rubate e pubblicate su Internet.
La top venti degli ultimi anni sono le seguenti:

123456 - password - 123456789 - 12345678 - 12345 - 111111 - sunshine - qwerty - iloveyou - princess - admin - welcome - 666666 - abc123 - football - 123123 - monkey - 654321 - !@#$%^&*

Utilizzo della stessa password
Il secondo caso è quando viene utilizzata la stessa password, benchè sicura, per tutti i siti, compresa la vostra banca on line.

In questo caso un attacco ad esempio a Facebook potrebbe permettere ad un hacker di ottenere la vostra login e password di accesso al noto social network. Se utilizzate le stesse credenziali per accedere anche alla vostra banca on line il guaio è fatto! L'esempio precedente non è casuale, nel settembre del 2018 Facebook è stata hackerata e sono stati **rubati dati di accesso di 50 milioni di utenti!**

Un altro meccanismo utilizzato dagli hacker per accedere alle vostre password è quello di mettervi in condizioni di fornirgliele voi stessi!
Ti sarà capitato di voler accedere ad un nuovo portale web e dover compilare i campi di nome, cognome, login, password etc. È frequente il caso che ci venga data la possibilità di accedere evitando questo passaggio, accredotandoci direttamente con le credenziali di Facebook. In questi casi siamo noi a fornire ai proprietari della nuova piattaforma i nostri dati di accesso.

Se la piattaforma venisse violata, o se essa stessa fosse stata creata da un haker, i nostri dati finirebbero velocemente nelle mani sbagliate. Purtroppo queste cose succedono molto più spesso di quanto crediamo.
La violazione di una password quindi può mettere seriamente in pericolo i nostri dati personali.
Non sottovalutate l'importanza di una loro corretta gestione.

Come scrivere password sicure

Così come ci sono modi per scoprire le password altrui, ci sono modi per rendere difficile l'identificazione di una password ben congegnata. Partiamo da quello che è meglio non fare:

- creare password corte con meno di 8 caratteri;
- creare password contenenti sequenze di numeri consecutive come 12345 oppure 987654;
- creare password con parole presenti nel vocabolario. Esistono attacchi specifici (attacchi a vocabolario) che riescono a scoprirle in pochissimo tempo;
- evitare password con sequenze di caratteri vicini nella tastiera. Una delle password più utilizzate è qwerty oppure asdf;
- evitate password contenenti la data di nascita vostra o dei vostri figli;
- contenenti il vostro nome o quello dei vostri figli;
- evitate di utilizzare la parola "password" o "pa$$w0rd".

Questi sono errori che la maggior parte di noi ha fatto prima di imparare a generare le password seguendo un criterio di generazione sicuro. Creare password sicure è più semplice di quanto si pensi e per farlo basta seguire queste semplici regole. Una buona password deve:

- deve essere lunga tra glii 8 e i 13 caratteri; più lunga è una password più risulta difficile da decifrare.
- deve contenere caratteri speciali come “! $ & + , - . / < > = ? @ ^ _ ~”; il loro utilizzo consente infatti di ampliare il numero di combinazioni, riducendo le probabilità di successo nella decifrazione da parte degli hacker;
- deve alternare lettere maiuscole e minuscole, anch’esse utili per introdurre un maggior numero di combinazioni;
- deve contenere numeri casuali e che non corrispondano a date a voi inerenti.

Crea le tue password sicure

Per creare password efficaci e allo stesso tempo facili da ricordare abbiamo bisogno di creare un sistema che ci permette di ricordarle con facilità e che siano facilmente modificabili. Così ci affideremo più che ad un insieme di numeri lettere e segni, useremo uno schema mentale che ci permetta di ricordarla facilmente.
Costruire una frase significa che solo noi la conosciamo ed equivale a creare una “matrice”, per esempio:

“Questa Password è Molto Sicura
Per Il Tuo Accesso Bancario On Line"

Usando solo le iniziali avremo: **“Qpemspitabol"**.

Possiamo renderla ancora più forte aggiungendo i caratteri speciali: ci basterà sostituire le lettere con caratteri speciali che le ricordano. Ad esempio si potrebbe sostituire la “a” con @ o la “i” con !, la “l” con il simbolo 1 e la “é“ con il simbolo “€“. Questa operazione si chiama di traslitterazione ovvero la sostituzione di un carattere con un altro. Così avremo ottenuto: **“Qp€msp!t@bo1"**

Questa è una password sicura! Hai imparato la tecnica della matrice. inizia a creare le tue matrici e differenziale a seconda degli account ai quali accedi. Il risultato sarà che anche se dovessero violare uno dei tuoi account gli altri non saranno compromessi.

PROTEGGERE LE NOSTRE PASSWORD SICURE

Custodite e proteggete i vostri dispositivi

Non lasciare i supporti come HD esterni o PC senza password. Approfittando di una tua assenza, chiunque potrebbe carpire informazioni preziose.

Non digitare le password in presenza di sconosciuti

è vero che i pallini oscurano le parole che si stanno digitando, ma almeno, l'ipotetico hacker saprà il numero di caratteri/cifre di cui si compone la password, se non addirittura carpire alcuni dei tasti digitati.

Fai attenzione con chi parli

Non essere troppo generoso di informazioni (quale banca on-line abbiamo, dove abitiamo, ecc.), a meno chè non ci si fidi dell'interlocutore. Molte volte è da queste informazioni che nascono fenomeni di phishing.

Questo messaggio si autodistruggerà in...

Passare al distruggi-documenti tutti i fogli su cui si trovano password, indirizzi ip, e quant'altro riguardi la sicurezza. Non lasciate traccia scritta delle vostre password, una volta imparata la matrice non ne avrete più bisogno.

WiFi Free solo se VPN

Assicurarsi che gli access point della vostra rete WiFi siano protetti da password particolarmente forti o abbiano un sistema di VPN (Virtual Private Network) che crea una rete parallela alla vostra (NowSpot Security)

ALLA FINE DELLA GIOSTRA

È giunto il momento di decidere da che parte stare

Come sempre abbiamo due modi di affrontare le cose: con consapevolezza, cercando di comprendere il mondo che viviamo; oppure evitando di guardare le cose, ficcando la testa sotto la sabbia nell'illusione che non ci sia nulla da guardare. I primi si assumono la responsabilità delle proprie azioni, cercano strumenti e strategie per migliorarsi e migliorare il proprio mondo; gli altri subiscono gli eventi come catastrofi, come eventi legati alla sfortuna o al caso. Due modi di vivere differenti, e nonostante si parli di nuove tecnologie, nessuno di questi è un comportamento nuovo. Esistono da quando esiste l'uomo. Jason Shogren ipotizza la scomparsa dell'uomo di Neandhertal. Nel suo studio avanza l'ipotesi che H.neanderthalensis si sia dovuto scontrare con la particolare cultura dell'H.sapiens (di cui siamo i discendenti): questa **cultura si basava su tecniche avanzate** di commercio, cosa che portava più tempo libero rispetto a una cultura basata sulla caccia. Il tempo libero ottenuto avrebbe permesso lo sviluppo di specializzazioni non strettamente legate alla sussistenza, come costruire utensili sempre più complessi o dedicarsi all'arte. La complessità e la versatilità di una tale cultura avrebbe avuto esito fatale per la più "tradizionale" cultura dei Neandertal.

Sta a noi decidere da che parte stare, sta a noi decidere se vogliamo adattare i nostri comportamenti alle nuove condizioni socio/economiche. Sta a noi decidere se integrarci o meno con una diversa modalità di vivere proposta dalla tecnologia.

Certamente un singolo individuo è libero di scegliere se accettare o meno questo "nuovo" sistema. Non è altrettanto libero di farlo un imprenditore, o un'azienda. Per questi c'è una ed una sola strada: guardare il mondo che li circonda e **mettere in campo tutti gli strumenti per esprimersi.** Così come chiamerebbe il fabbro per costruire i cancelli che tutelano lo spazio fisico della produzione, così si assicura la conoscenza dei tecnici informatici capaci di mantenere in sicurezza rapporti e reti digitali.

Nowtech

Una storia lunga 35 anni

Nowtech nasce nel 1984, da allora si occupa di meccanizzazione e informatizzazione dei flussi di produzione aziendali. L'azienda condotta da Antonio Aprea ha passato le diverse "ere" dell'informatizzazione mantenendo sempre alto il livello di preparazione e offrendo ai propri clienti i processi più evoluti possibili per le tecnologie a disposizione, grazie alla curiosità del suo fondatore.

Siamo un provider di soluzioni di connettività e di informatizzazione destinato alla PMI. Crediamo che la risposta alle esigenze del cliente può solo venire da soluzioni appositamente bilanciate per la singola azienda. Studiamo le esigenze, le caratteristiche aziendali, le procedure di acquisizione e gestione dei dati proponiamo le soluzioni "cucite" apposta per il cliente. **Ottimizzare le risorse e massimizzare i risultati** sono i primi obiettivi che perseguiamo.

Attraverso un'offerta verticale forniamo soluzioni che consentono alle aziende di conquistare autonomia nel panorama commerciale attuale. Partendo dalla connettività offriamo la possibilità di sganciare le imprese dalla dipendenza ai grandi provider monopolisti della connettività. Il libero mercato ha creato opportunità da cogliere per migliorare efficienza e dinamicità.

Grazie al reparto di sviluppo interno Nowtech propone soluzioni per tutte le esigenze di informatizzazione e gestione dei dati prodotti dalla attività aziendale. Software di gestione, CRM e sistemi di sicurezza e le soluzioni

voip siamo vicini alle aziende in un rapporto di partnership rivolto alla semplificazione delle procedure ed alla crescita dell'efficienza.

OGGI NOWTECH È UN FULL PROVIDER DI SERVIZI INFORMATICI

Promuove sistemi di connettività indipendente e soluzioni Voip avanzate, software di gestione, piattaforme di collaborazione e soluzioni per la sicurezza informatica.

Il punto di forza di NOWTECH è sicuramente la capacità di **entrare in sintonia con le strutture produttive** e fornire consulenza finalizzata alle soluzioni più adatte alle singole esigenze.
L'assistenza è il nostro punto focale, per questo abbiamo scelto di gestire direttamente ed internamente il reparto, crediamo nel rapporto diretto tra sviluppatore ed utilizzatore delle soluzioni proposte.

“Riuscire ad apprezzare
il dolce naufragar
del mare di internet,
e possibile solo
creando e stimolando consapevolezza
sulla sua potenzialità e immensità”
Antonio Aprea