

Il concetto di sicurezza informatica nell'ottica del GDPR

Ing. Marino Pietro
Azienda: Remedios Tecnologia

Nell'ottica del regolamento europeo n. 2016/679 (GDPR) questo concetto di sicurezza informatica ha assunto un significato più attuale alla luce anche dei sempre più numerosi attacchi ed incidenti di natura informatica che lasciano intuire una preoccupante tendenza alla crescita di tale fenomeno.

In particolare negli ultimi tempi si è assistito ad una rapida evoluzione della minaccia che possiamo definire “cibernetica” che è divenuta un bersaglio specifico per alcune tipologie di attaccanti particolarmente pericolosi.

I pericoli legati a questo genere di minaccia sono particolarmente gravi per due ordini di motivi:

- il primo è la quantità di risorse che gli attaccanti possono mettere in campo, che si riflette sulla sofisticazione delle strategie e degli strumenti utilizzati;
 - il secondo è rappresentato dal fatto che il primo obiettivo perseguito è il mascheramento dell'attività, in modo tale che questa possa procedere senza destare sospetti.
-

Per mantenere la sicurezza e prevenire trattamenti in violazione al GDPR, il titolare del trattamento o il responsabile del trattamento deve valutare anche il rischio informatico che può essere definito come il rischio di danni economici (rischi diretti) e di reputazione (rischi indiretti) derivanti dall'uso della tecnologia, intendendosi con ciò sia i rischi impliciti nella tecnologia (i cosiddetti rischi di natura endogena) che i rischi derivanti dall'automazione, attraverso l'uso della tecnologia, di processi operativi aziendali (i cosiddetti rischi di natura esogena).

In particolare questi ultimi possono essere:

- danneggiamento di hardware e software;
 - errori nell'esecuzione delle operazioni nei sistemi;
 - malfunzionamento dei sistemi;
 - programmi indesiderati.
-

Nel GDPR un chiaro riferimento alle misure di sicurezza già si trova nell'art. 22 quando si chiarisce che il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento dei dati personali è effettuato conformemente al Regolamento (principio di accountability).

La guida completa per la sicurezza informatica delle piccole e medie attività – 2018

**THE COMPLETE
CYBERSECURITY
GUIDE FOR SMALL
AND MEDIUM
BUSINESSES**



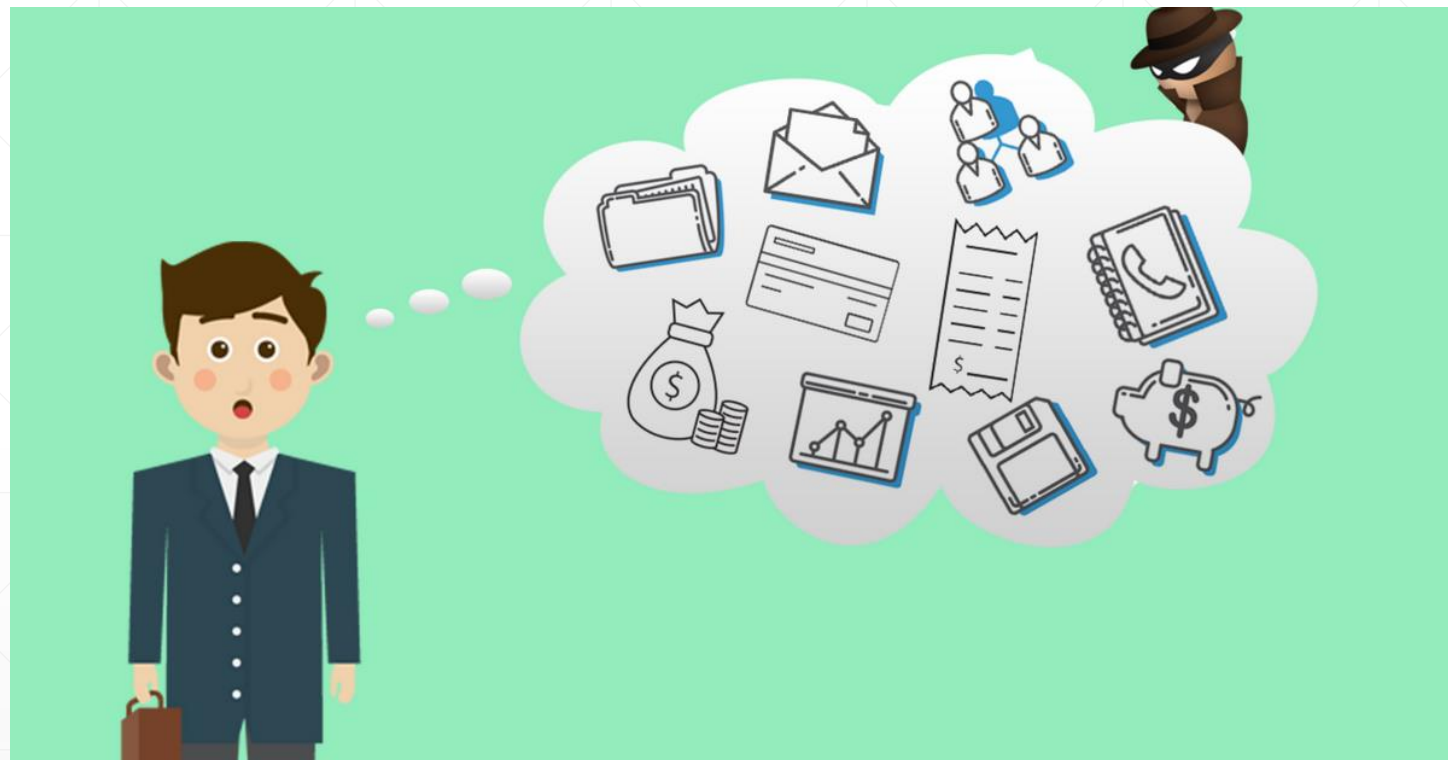
1. Definisci le tue vulnerabilità

Il primo step per proteggere te stesso dalle minacce alla sicurezza informatica è quello di definire le tue vulnerabilità. Se non sai quali sono le tue debolezze, come puoi sistemarle? Se non sai che tipo di dati conserva la tua società, come puoi proteggerli?

Inizia a individuare le “pietre preziose” dei tuoi dati aziendali. Quali sono i dati più importanti della tua società?

Potrebbe essere qualsiasi cosa, dalla proprietà intellettuale ai dati dei clienti, inventari, informazioni finanziarie, ecc. Dove conservi tutti questi dati? Una volta trovata la risposta a queste domande, puoi iniziare a pensare ai rischi cui sono esposti i tuoi dati.

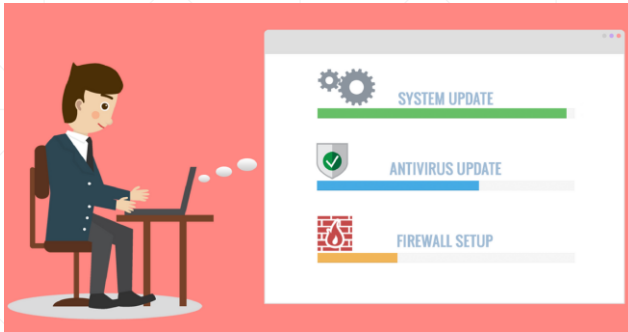
Fai una mappa accurata di tutte le procedure seguite da te e dal tuo personale per raccogliere, conservare e divulgare questi dati. Pensa a tutti questi punti di transito lungo il percorso attraverso cui è possibile perdere i dati. Considera le conseguenze di una violazione della sicurezza informatica per te, per i tuoi dipendenti, clienti e partner commerciali. Dopo aver fatto ciò, puoi iniziare a mettere in pratica le precauzioni.



2. Proteggi i tuoi computer e dispositivi

I tuoi computer e altri dispositivi sono i portali attraverso cui svolgi la tua attività. Ma dato che questi dispositivi sono collegati a Internet e a una rete locale, sono vulnerabili all'attacco. Queste sono le nostre linee guida per migliorare la sicurezza nei sistemi dei computer della tua società.

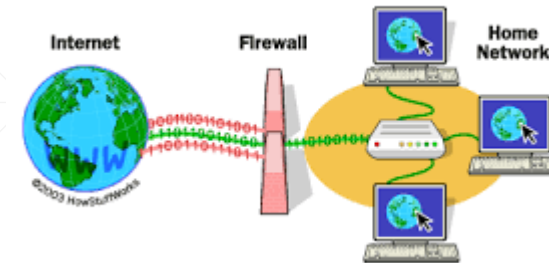
A. Aggiorna il tuo software



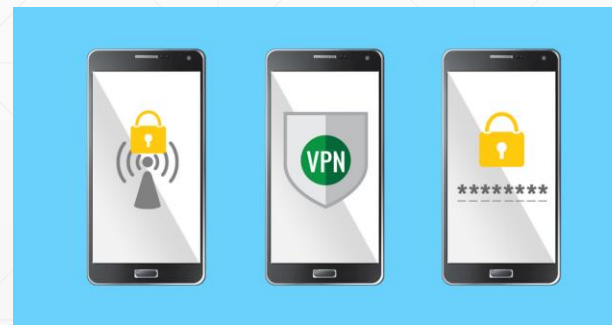
B. Proteggi contro i virus



C. Imposta un firewall



D. Precauzioni speciali per portatili e altri dispositivi mobili



A. Aggiorna il tuo software



Il primo vero step (e probabilmente il più semplice) per garantire che i tuoi sistemi non siano vulnerabili all'attacco, è di usare sempre la versione del software più aggiornata su cui può contare la tua attività. I pirati informatici trascorrono il loro tempo a ricercare bug nei software popolari, scappatoie per entrare nel sistema. Lo fanno per qualsiasi motivo: per fare soldi, per dichiarazioni politiche o semplicemente perché possono farlo. Questo tipo di intrusione può causare danni incalcolabili alla tua attività. I pirati informatici possono rubare il numero della carta di credito dei tuoi clienti dal tuo sito web, oppure rubare le password dal tuo computer. Se ciò accade, la tua attività è davvero nei guai.

Microsoft e altre società di software sono sempre alla ricerca delle vulnerabilità del loro software. Quando ne trovano una, lanciano un aggiornamento affinché gli utenti effettuino il download. Scaricare questi aggiornamenti non appena vengono lanciati è molto semplice, ci si chiede perché molte attività non sono molto attente in merito.

Nel 2017, un attacco globale ransomware chiamato "WannaCry", ha colpito migliaia di vittime, incluse grandi organizzazioni come FedEx e il Servizio sanitario nazionale del Regno Unito (leggi altro su ransomware qui sotto). Prima dell'attacco, Microsoft aveva lanciato un patch, l'aggiornamento di un software che risolve il problema, ma molti amministratori di sistema non l'hanno installato, portando così a un attacco massiccio. Fortunatamente l'attacco fu arrestato. Ma non è sempre così. Il metodo più semplice per evitare di diventare la prossima vittima dei pirati informatici è di aggiornare coscientemente il software.

B. Proteggi contro i virus

I virus sono programmi dannosi che infettano il tuo computer senza alcun preavviso. I virus possono dare molte cose, ma di solito hanno accesso ai tuoi file e li cancellano o modificano. I virus si diffondono velocemente moltiplicandosi e inviandoli alle persone presenti nella tua lista di contatto. Se un computer nella tua rete riceve un virus, può diffondersi velocemente in tutta la tua società, causando una significativa perdita di dati. Se comunichi con i tuoi clienti tramite email (proprio come facciamo tutti), corri il rischio di infettarli.

I malware e i ransomware sono le due tipologie di virus in assoluto più pericolose. Esistono alcune differenze tra i malware e i ransomware. Malware significa “software dannoso”. Funziona spingendo la vittima a scaricare un dato software per avere così accesso al computer della vittima. Può rilevare gli accessi effettuati dal tuo computer, informazioni sensibili oppure diffondere spam tramite email.

Ransomware è uno specifico tipo di malware. Blocca il tuo computer e ti impedisce di accedere ai tuoi file importanti fino a quando non paghi il ransom. Ransomware funziona crittografando i tuoi file attraverso una chiave privata accessibile solo ai suoi creatori. L'attacco WannaCry citato sopra è stato un tipo di ransomware. Pagare il ransom non necessariamente aiuta: non c'è alcuna garanzia che i pirati informatici sbloccheranno davvero i tuoi file.

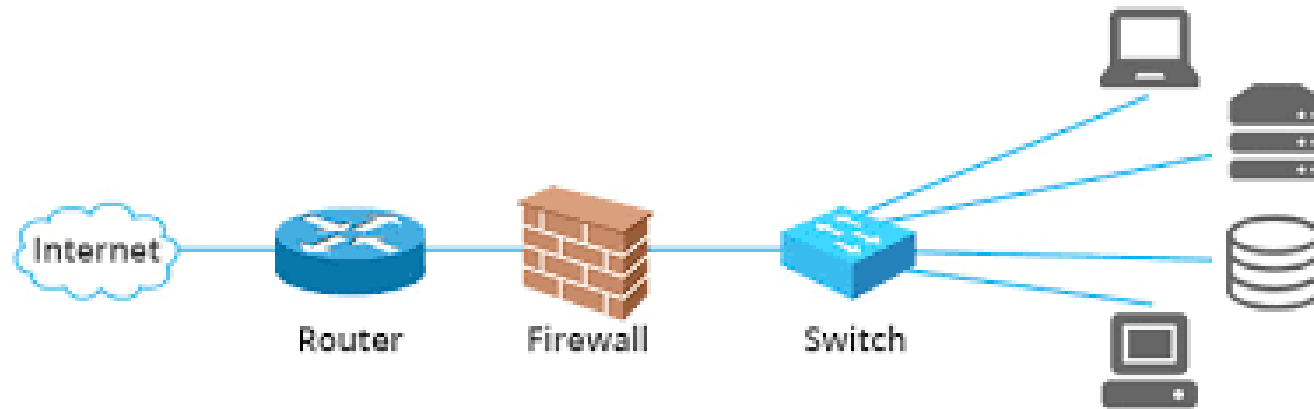
Ci sono vari step di base che puoi seguire per evitare di infettare il tuo computer con i virus. Innanzitutto, installa un software antivirus su tutti i computer dell'ufficio. Il software antivirus scansione i messaggi email in entrata, così come i file attualmente sul tuo computer, e poi elimina o mette in quarantena tutti i virus che trova. I pirati informatici cercano sempre di inserire nuovi virus, pertanto bisogna aggiornare regolarmente il software antivirus. I migliori provider di software comprendono una funzione che comanda il tuo computer a scaricare gli aggiornamenti automaticamente. Devi accertarti che il tuo personale non apra i file sospetti, ed elimini qualsiasi allegato proveniente da una fonte non affidabile.

L'utilizzo di una VPN per accedere a Internet può fornirti anche una spinta extra alla sicurezza. Dato che le VPN ti consentono di accedere a Internet in modo anonimo, e dato che criptano tutti i tuoi dati, rendono molto difficile il rilevamento del tuo computer da parte dei pirati informatici. Buoni provider di VPN ti inviano un avviso di sicurezza quando cerchi di accedere a URL sospetti.

Se sei già stato vittima di un attacco ransomware, non è troppo tardi. Questa guida passo dopo passo ti aiuterà a sconfiggere l'attacco.



C. Imposta un firewall



Come nella maggior parte delle attività, tutti i dispositivi presenti nel tuo ufficio sono probabilmente collegate a una connessione internet a banda larga sempre attiva. In tal caso, allora, c'è una forte probabilità che i pirati informatici abbiano sondato la tua rete almeno una volta. I pirati informativi lo fanno in modo random, ma quando trovano un indirizzo valido, sfruttano tutte le vulnerabilità per accedere alla tua rete e ai singoli computer presenti su tale rete.

Installare un firewall è il modo migliore per evitare che si verifichi questo tipo di attacco. I firewall funzionano separando diverse parti della rete dalle altre, consentendo solo il passaggio di traffico autorizzato attraverso le zone protette della rete. Se gestisci una piccola attività, il tuo firewall delimiterà la tua rete locale privata dal più ampio internet. Un buon firewall esamina tutti i pacchetti di dati che entrano nella tua rete per accertarne la legittimità e per filtrare quelli sospetti. Per evitare che i pirati informatici attacchino i singoli computer della tua rete, il firewall oscura l'identità di ogni computer.

L'installazione di un firewall è complessa e deve essere svolta solo da personale qualificato. Ciò facilita il tuo lavoro: tutto ciò che devi fare è parlare al tuo amministratore di sistema e accertarti che la tua rete sia protetta.

D. Precauzioni speciali per portatili e altri dispositivi mobili

Dato che sono portatili e che quindi possono uscire dall'ufficio, i portatili sono particolarmente a rischio per violazioni della sicurezza. Sono un bersaglio per i ladri perché sono facili da rubare e vendere. I dipendenti possono anche non prestare molta attenzione dato che la maggior parte delle società sostituisce la macchina in caso di perdita o furto. Tuttavia, sostituire un portatile comporta un notevole esborso finanziario, soprattutto per una piccola attività. Ma questo non è il problema maggiore. I portatili del personale, soprattutto quelli del personale più anziano, molto probabilmente contengono delle informazioni sensibili che possono danneggiare la tua attività se finiscono nelle mani sbagliate.

Ci sono alcune precauzioni che tu e il tuo personale dovete prendere per evitare il furto dei portatili e per mitigare le conseguenze più gravi se una società perde un portatile. Innanzitutto, quando un dipendente utilizza un portatile in un'area pubblica, o anche durante un meeting o una conferenza, deve sempre accertarsi di tenerlo a vista. I portatili devono essere inseriti nel bagaglio a mano e non lasciati nell'area di deposito bagagli presso hotel o aeroporti.

I pirati informatici possono anche accedere facilmente ai dati di un computer o dispositivo mobile se la connessione è su una rete non sicura. Esistono varie misure che consigliamo per proteggere i dati, come l'utilizzo di una password forte, il backup di tutto il lavoro fatto sul portatile prima di un viaggio e la crittografia dei dati. Queste linee guida riguardano appositamente i portatili. Li analizzeremo ulteriormente nella sezione 3 "Proteggi i tuoi dati".

Bisogna pianificare in anticipo la protezione dei dispositivi della società. Se utilizzi una soluzione cloud per una qualsiasi esigenza di software, guarda all'interno delle funzioni di gestione del dispositivo mobile del tuo provider. I principali provider di cloud computing ti consentono di eliminare un account da qualsiasi dispositivo che scompare.

Tutti questi consigli si applicano anche ai cellulari aziendali. Esistono vari step da seguire per mettere al sicuro i cellulari aziendali e questa guida specifica per iPhone ti accompagnerà in questa procedura. Ci sono varie app sulla sicurezza che consigliamo di usare, così come dei metodi per modificare le impostazioni del tuo telefono per renderle più sicure.

Uno dei modi migliori per proteggere i dispositivi, siano essi portatili, cellulari, dispositivi Alexa di Amazon, o anche PS4 in ufficio (se hai un ufficio divertente con un dispositivo di gioco!), è quello di installare una VPN per crittografare tutti i dati che passano attraverso questi dispositivi. Non c'è necessariamente bisogno di installare una VPN su ogni dispositivo; invece puoi installarlo direttamente sul tuo router dell'ufficio. In questo modo, tutti i dispositivi che utilizzano la connessione internet dell'ufficio saranno protetti.

È inoltre importante creare una policy su quali dispositivi il personale può portare a lavoro. Molte società incoraggiano i lavoratori a portare i loro portatili e altri dispositivi in ufficio poiché questo metodo è più economico del fornire ad ogni dipendente l'attrezzatura aziendale. Consigliamo di chiedere di utilizzare tutti i dispositivi personali per qualsiasi lavoro per installare software antivirus e ricevere aggiornamenti regolari.

3. Proteggi i tuoi dati

A prescindere dal tipo di attività che gestisci, i tuoi dati sono davvero la parte centrale di ciò che fai. Senza le informazioni di contatto dei clienti, inventari, dati di proprietà e tutto il resto, non saresti in grado di funzionare come attività. Puoi perdere i tuoi dati in qualsiasi modo. Il tuo hardware può essere danneggiato o rotto, i pirati informatici possono entrare nel tuo sistema e violarlo, oppure potresti essere colpito da un disastro naturale. Il tuo obiettivo dunque dovrebbe essere quello di assicurarti contro la perdita di dati prendendo delle precauzioni contro i suoi effetti peggiori.

A. Mettere in atto una procedura per il backup dei dati fondamentali



B. Cripta i dati sensibili della società conservati su cloud



C. Proteggi le tue password



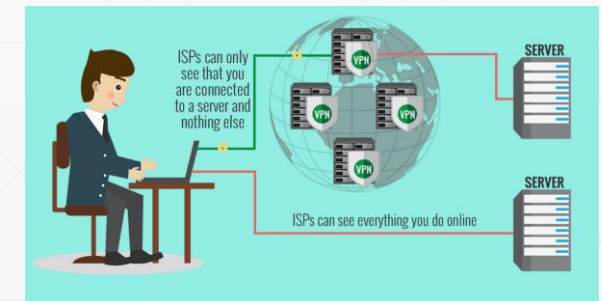
D. Stabilisci delle autorizzazioni



E. Proteggi le tue reti wireless



F. Naviga su Internet in modo sicuro



3. Proteggi i tuoi dati

A prescindere dal tipo di attività che gestisci, i tuoi dati sono davvero la parte centrale di ciò che fai. Senza le informazioni di contatto dei clienti, inventari, dati di proprietà e tutto il resto, non saresti in grado di funzionare come attività. Puoi perdere i tuoi dati in qualsiasi modo. Il tuo hardware può essere danneggiato o rotto, i pirati informatici possono entrare nel tuo sistema e violarlo, oppure potresti essere colpito da un disastro naturale. Il tuo obiettivo dunque dovrebbe essere quello di assicurarti contro la perdita di dati prendendo delle precauzioni contro i suoi effetti peggiori.

G. Proteggi i dati sensibili creati da lavoratori a distanza e lavoratori in movimento



H. Proteggi i dati dei tuoi clienti



A. Mettere in atto una procedura per il backup dei dati fondamentali

Esistono due diverse tipologie di backup. Quando effettui un backup completo, fai una copia di tutti i dati che hai selezionato e lo metti su un altro dispositivo oppure lo trasferisci su uno strumento diverso. Con un backup incrementale, invece, aggiungi semplicemente i dati che hai creato dall'ultima volta che hai effettuato il backup del tuo sistema.

Il metodo più semplice ed efficiente è dato dalla combinazione di entrambi. Effettua periodicamente un backup completo e un backup incrementale ogni giorno. Oppure puoi effettuare un backup completo ogni notte dopo l'orario di lavoro. È fondamentale testare il funzionamento dei backup: perdere tutti i dati e scoprire che i backup non funzionano, sarebbe una tragedia. È possibile farlo ripristinando una porzione di test dei tuoi dati in una nuova location. In questo modo sarai certo che i tuoi backup funzionano e ti aiuteranno a identificare qualsiasi problema nella procedura di backup.

Esistono molti modi diversi per il backup dei tuoi dati. Puoi inserirlo in un dispositivo fisico, come una penna USB o un secondo hard disk, oppure posizionarlo in una cartella condivisa sulla tua rete. Puoi mantenere i backup al sicuro in location esterne. Tuttavia, facendo il backup dei tuoi dati su una specifica location fisica non ti aiuterà in caso di disastro naturale o furto. Consigliamo vivamente a tutte le società di investire in sistemi di backup su cloud. Per ulteriori dettagli, consulta la prossima sezione.



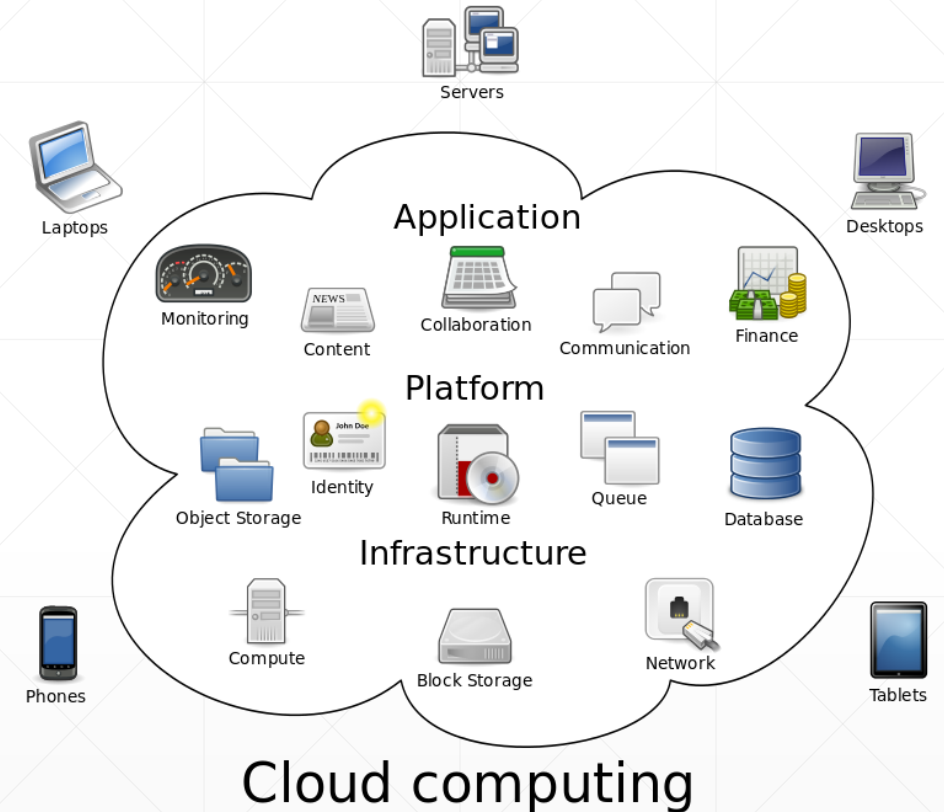
B. Cripta i dati sensibili della società conservati su cloud

Oggi, molte società conservano la maggior parte, se non tutti, i loro dati su una piattaforma su cloud. Questo può essere un sistema di memoria su cloud come Dropbox, o una piattaforma SaaS (software come un servizio) come Salesforce. Dato che facciamo riferimento a questi sistemi come “cloud”, tendiamo a immaginare che i nostri dati non siano conservati sul tuo hard disk o sulla tua rete locale, ma piuttosto su strutture computerizzate da remoto fornite dal sistema su cloud. È pertanto fondamentale analizzare le misure di sicurezza che il tuo provider cloud ha messo in atto e se i dati sono protetti a livello adeguato.

Esistono vari approcci da poter intraprendere per essere certi della sicurezza dei tuoi file su cloud. L'approccio più semplice e sicuro è quello di crittografare manualmente i file e ci sono vari programmi che ti aiutano in questa direzione. Questo non significa che non devi fare affidamento sulla sicurezza del provider cloud, e puoi usarlo senza preoccuparti. Basta accertarsi di non caricare le tue chiavi di crittografia.

Detto ciò, bisogna indagare attentamente le opzioni di memoria su cloud. Ci sono molti provider sul mercato, e alcuni tra quelli più piccoli e meno conosciuti hanno in realtà delle strutture di sicurezza più solide dei grandi nomi. Alcuni di questi servizi crittograferanno automaticamente i tuoi file prima di caricarli su cloud.

Un'altra opzione è quella di usare BitTorrent Sync, che è un servizio totalmente gratuito. BitTorrent Sync è stato progettato come sostituto per i sistemi su cloud ma in realtà non memorizza i file su cloud. Ti consente invece di collaborare su documenti attraverso una piattaforma di condivisione dei file (P2P) peer-to-peer. Questi servizi tendono a utilizzare il livello di crittografia più alto AES-256 e attiva un'autenticazione a due fattori, che aggiunge un ulteriore livello di sicurezza.



C. Proteggi le tue password

Il modo più comune per autenticare l'identità è accedere alla tua rete o ai tuoi dati importanti attraverso una password. A differenza degli altri sistemi di autenticazione high-tech come smart card, e impronte digitali o scansioni dell'iride, le password sono utili perché non costano nulla e sono facili da usare. Tuttavia, le password sono anche aperte agli attacchi. I pirati informatici hanno sviluppato degli strumenti sofisticati e automatizzati che consente loro di craccare password semplici in pochi minuti. Possono utilizzare anche vari metodi fraudolenti per accedere alle password della tua società, come un attacco phishing, in cui si travestono da strutture ufficiali (come Google) e ingannano le persone a fornire le loro password.

Le password possono diventare inefficaci per svariati motivi. Spesso, trascuriamo di proteggere i nostri documenti sensibili con una password, questo significa che chiunque si siede davanti al tuo computer può avere accesso a tali documenti. Per evitare di dimenticare le password, molti dipendenti le scrivono in bella vista. E, cosa ancora più cruciale, le persone tendono a utilizzare password deboli, facili da ricordare, usano la stessa password tantissime volte senza mai cambiarle. Tutti questi errori lasciano la porta aperta ai pirati informatici.

Questi sette step per creare una password forte aiuteranno a evitare attacchi informatici:

- Creare password diverse per servizi diversi
- Modificare regolarmente le password
- Scegliere una password forte
- Optare per una verifica a due step
- Disattivare il completamento automatico per username e password
- Utilizzare un manager di password, un'app o un programma che conserva in modo sicuro tutte le password dell'utente
- Non inviare la tua password tramite email o tramite telefono

Creare una password più forte non è così difficile. Usare uno strumento di password, come questo, che ti dice quanto è buona una password e quanto tempo ci vuole affinché i pirati informatici possano craccarla. Puoi anche utilizzare un generatore di password random sicuro che creerà una password completamente random.

Educare lo staff sull'importanza di password forti è fondamentale se vuoi che le password rappresentino uno strumento chiave nel tuo arsenale per la sicurezza informatica, piuttosto che una scappatoia percorribile dai pirati informatici.



D. Stabilisci delle autorizzazioni



Se pensi a chi ha accesso alle informazioni sensibili nella tua società, la risposta è probabilmente troppe persone. Segui gli step per limitare l'accesso al tuo sistema. Solo quei membri dello staff che sono autorizzati a gestire il tuo sistema e installare il software, devono avere accesso agli account amministrativi.

Le società possono anche essere negligenti consentendo a molteplici membri del personale di condividere login e password. In questo modo è impossibile definire come o quando si è verificata una violazione nel sistema. Dai a ogni utente il suo account, attivando autorizzazioni specifiche per il suo lavoro. Se stai utilizzando Windows, puoi assegnare diversi livelli di autorizzazioni sulla base dei ruoli all'interno della tua società. Se un membro dello staff è assente da molto tempo, oppure ha lasciato la tua società, revoca l'accesso e le autorizzazioni, il prima possibile.

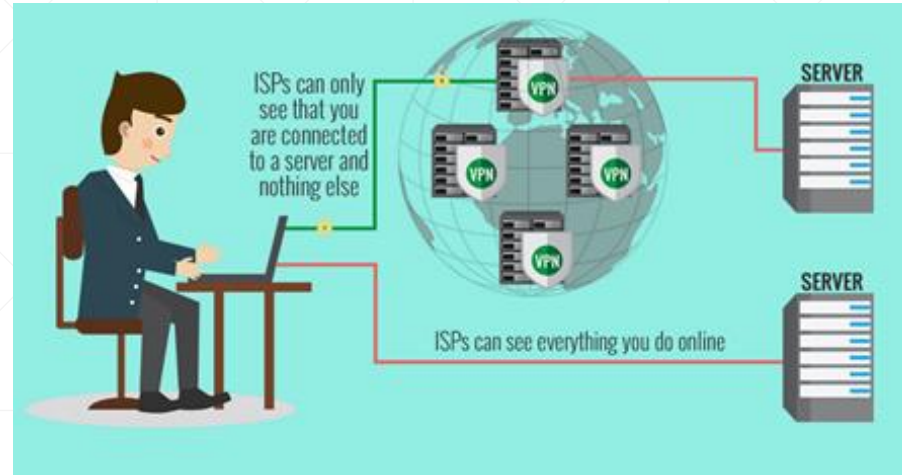
E. Proteggi le tue reti wireless



Un altro modo in cui i pirati informatici possono entrare nel tuo sistema è attraverso una rete wireless nel tuo ufficio. Dato che le reti Wi-Fi usano un link radio piuttosto che cavi per collegare i computer a internet, tutto ciò che ci vuole è spostarsi nel range radio della tua rete oltre a qualche strumento gratis per irrompere. I ladri che hanno accesso alla tua rete possono rubare i tuoi file e danneggiare i tuoi sistemi. Anche se i dispositivi Wi-Fi sono attivi con le funzioni di sicurezza per evitare che ciò accada, la maggior parte di queste funzioni sono disattivate di default per semplificare la procedura di configurazione.

Se stai utilizzando una rete Wi-Fi, accertati di attivare queste funzioni di sicurezza. Puoi anche restringere l'accesso wireless all'orario di ufficio in modo che i pirati informatici non possano entrare nel tuo sistema durante la notte. Puoi anche evitare ai passanti l'accesso alla tua connessione limitando l'accesso Wi-Fi a specifici computer impostando dei punti d'accesso.

F. Naviga su Internet in modo sicuro



Quando tu e i membri del tuo staff navigate su internet, le tue attività possono essere monitorate in una molteplicità di modi piccoli e impercettibili. Queste attività possono quindi essere aggredite da agenti esterni senza il tuo consenso. I tuoi dipendenti possono navigare inavvertitamente su siti pericolosi che rubano i dati della tua società. E le tue informazioni personali e aziendali possono essere compromesse se si entra nei siti web con una connessione non crittografata.

Il modo migliore per crittografare la tua connessione e garantire la privacy delle tue attività e la privacy personale dei tuoi dipendenti è quello di installare una VPN. Una VPN, o una rete virtuale privata, maschera l'indirizzo IP della tua società e cripta i tuoi dati di navigazione. Rende anonimo la tua navigazione, il che può essere importante se la tua attività ricerca frequentemente competitor, o se lo storico aggregato di navigazione può rivelare le informazioni di proprietà dei concorrenti.

Il lato negativo per usare una VPN è che i servizi VPN affidabili e ricchi di funzioni hanno un costo di abbonamento mensile. Molti individui e società hanno optato per l'utilizzo di una web proxy gratis come alternativa. Il problema è che non sappiamo esattamente chi sta operando le proxy disponibili online gratis. Possono essere davvero hackerate, oppure essere utilizzate per la raccolta da parte di varie entità pubbliche e private. Mentre una proxy nasconde la tua identità e l'attività dei siti che visiti, può vedere potenzialmente tutto ciò che fai online. Questo è uno dei motivi per cui consigliamo di investigare in una VPN piuttosto che in una proxy, per una navigazione davvero sicura.

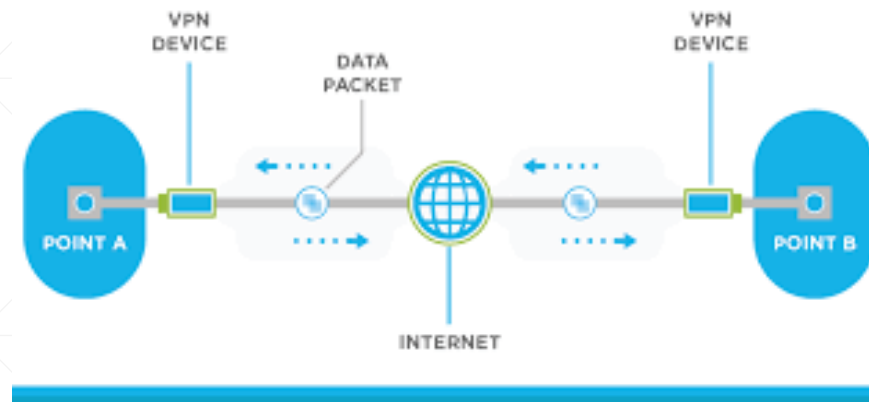
Puoi sostenere la sicurezza anche aggiungendo varie funzioni al tuo browser. Dato che il browser Firefox è open-source, nel tempo è stato creato un gruppo robusto di componenti aggiuntivi di sicurezza. Ciò comprende blocchi per gli annunci pubblicitari, protezione dei dati del browser, cookie, manager di cache e altro. Per ulteriori informazioni, controlla l'elenco completo dei 20 componenti aggiuntivi per la sicurezza di Firefox.

G. Proteggi i dati sensibili creati da lavoratori a distanza e lavoratori in movimento

Molte piccole attività collaborano con lavoratori a distanza per l'esecuzione di un'ampia gamma di attività. Con internet, lavorare con gli altri in giro per il mondo, è facile. Assumere lavoratori a distanza comporta svariati vantaggi: significa che non devi assumere un impiegato che si prenda cura di una specifica attività tecnica, e che inoltre ti apri a un ampio range di candidati qualificati. Tuttavia, il lavoro a distanza comporta qualche ostacolo alla sicurezza informatica. Devi aver implementato tutte le protezioni analizzate, ma molte vengono rese inefficaci se i lavoratori a distanza accedono ai tuoi dati sensibili al di fuori della rete protetta della società, soprattutto se utilizzano un hotspot Wi-Fi pubblico.

Una soluzione per la gestione dei dispositivi mobili, come descritto nella sezione 2.D., può aiutare a gestire i lavoratori a distanza, così come i dipendenti che viaggiano per lavoro. La cosa più importante è che devi garantire che se i lavoratori a distanza accedono ai dati sensibili della società, lo fanno attraverso la rete protetta della società con una connessione sicura.

Windows offre una connessione su desktop da remote, ma ciò in sé non è sufficiente per garantire i tuoi dati. Se fai affidamento sui lavoratori a distanza, e se non puoi permetterti la perdita di dati, è importante implementare una VPN specializzata che consente agli utenti a distanza di entrare nella rete dell'ufficio, dopo di che possono collegarlo alle loro macchine utilizzando delle funzioni di connessione da remoto su desktop. Ciò può diventare complesso, quindi parla con il tuo tecnico per vedere se può configurare una VPN specifica per la tua rete.



H. Proteggi i dati dei tuoi clienti

Una cosa è se i dati sensibili della tua società vengono persi, altro è compromettere i dati dei tuoi clienti. Ciò comporta diverse conseguenze legali, pertanto bisogna trattare le informazioni sensibili dei clienti con la massima attenzione.

Generalmente, i dati dei clienti passano attraverso vari punti. Se gestisci un sito di ecommerce o altre procedure di pagamento attraverso il tuo sito web, il primo transito delle informazioni sensibili (inclusi nomi e dati delle carte di credito) è dal browser web del cliente al server web dell'ecommerce. Il modo migliore per proteggere questi dati è assicurarsi che il sito web utilizzi un certificato SSL e un protocollo HTTPS, almeno nelle pagine che raccolgono dati sensibili. In questo modo si garantisce che i dati dei clienti vengono criptati quando si passa da un server all'altro. Se stai trasferendo i dati dei clienti all'interno della società, bisogna applicare tutte le funzioni di sicurezza descritte sopra, soprattutto quelle relative alla memoria cloud e al trasferimento.



4. Infondi la cultura della sicurezza informatica sul tuo luogo di lavoro

Le misure sottolineate in questa guida sono complete, e se segui tutte le linee guida relative alla tua attività, abbasserai considerevolmente il rischio di un attacco informatico. Questo è quanto, se l'attività è tua.

Tutto quello che serve è inviare i dati ai clienti su una connessione non sicura oppure cliccare su un link non sicuro e scaricare malware, per far sì che tutti i sistemi di sicurezza e tutti gli sforzi fatti vadano persi. Ecco perché la misura più importante è quella di educare il tuo staff sull'importanza della sicurezza informatica.

Dall'altro lato, se infondi una cultura della sicurezza informatica nel tuo luogo di lavoro, se spieghi la politica della sicurezza informatica e il perché, e se formi il tuo staff a gestire l'hardware e i dati della società in modo sicuro, i tuoi dipendenti diventeranno la tua prima, e più efficace, linea di difesa contro gli attacchi informatici.

Il modo migliore per far sì che i tuoi dipendenti entrano nel piano della sicurezza informatica è quello di progettare in collaborazione con loro. Coinvolgendoli nel piano, si aumenta la motivazione. I membri del tuo staff sono anche esperti della tua attività, dei suoi punti di forza e di debolezza. Sono coloro che lavorano con i dati sensibili della società, quindi sanno quali sono le vulnerabilità e quali sistemi bisogna rafforzare o migliorare.

Inizia a tenere delle sessioni regolari di formazione con il tuo staff sui problemi della sicurezza informatica. Questo è un sistema metodologico attraverso tecniche di sicurezza come quelle di cui abbiamo parlato. Assicurati che le password e le autorizzazioni siano aggiornate e che utilizzano password impossibili da craccare. Accertati di non far lasciare password in giro. Mostra loro come evitare attacchi phishing tramite email e i rischi di malware da siti web pericolosi. Insegna ai tuoi dipendenti i tanti modi in cui i pirati informatici cercano di ottenere le informazioni. Incoraggiali a non parlare in pubblico delle informazioni riservate della società, non si sa mai con chi si può parlare e chi sta ascoltando. Assicurati che queste linee siano facili da comprendere e da seguire. Abbiamo creato una stampa comprendente semplici step. Puoi appendere questo schema su una bacheca, un frigo, oppure personalizzarlo per adattarlo alle tue esigenze specifiche.

Inserisci i principi della sicurezza informatica in una policy scritta, e falla firmare ai tuoi dipendenti, accertandoti che abbiano capito l'importanza della sicurezza informatica. Puoi anche inserire questi elementi nel contratto del tuo personale.

La cosa importante da ricordare è che queste minacce cambiano di continuo. I pirati informatici hanno sempre metodi più creativi e più sofisticati per violare i computer e rubare i dati. Mantieniti aggiornato con gli sviluppi della sicurezza informatica, e assicurati di formare il tuo staff anche su questi progressi.



GRAZIE

Ing. Marino Pietro

Remedios Tecnologia

Riferimenti:

VpnMentor

GDPR gazzetta ufficiale