+ Windows 10

MANUALE OPERATIVO DI SICUREZZA INFORMATICA

Dieci passaggi che ogni azienda dovrebbe adottare per proteggersi dagli attacchi informatici

Più protezione, dall'accensione allo spegnimento

Il panorama della sicurezza informatica è in costante cambiamento ed espansione. Le piccole e medie imprese devono confrontarsi sempre più spesso con attacchi che minacciano le loro informazioni e i dati privati dei clienti. Questa guida è ideata per aiutare le piccole e medie imprese con risorse IT limitate a rafforzare subito la sicurezza informatica, con poca o nessuna spesa.

SOMMARIO

Il panorama delle minacce

Tendenze di sicurezza informatica nelle piccole e medie imprese

Queste sono cinque tendenze principali nello stato della sicurezza informatica per le piccole e medie imprese, secondo il Ponemon Institute[1]:

1. **Sempre più aziende sono sotto attacco.**
Negli ultimi 12 mesi, gli attacchi informatici ai danni delle piccole e medie imprese sono aumentati dell'11%, passando dal 55 al 61%. I principali attacchi contro le piccole aziende sono di tipo phishing/ingegneria sociale (48%) e basati sul Web (43%). Allo stesso tempo, gli attacchi informatici diventano sempre più mirati, gravi e sofisticati.

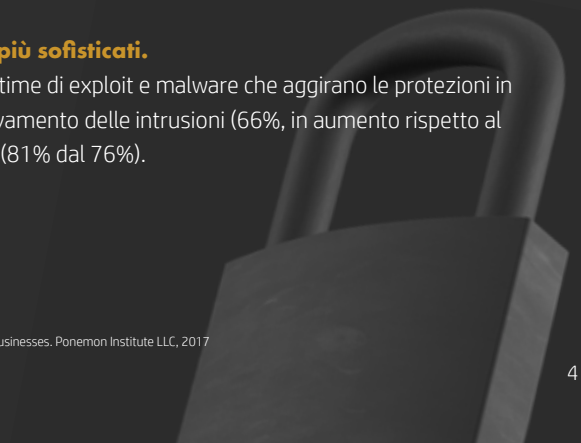
2. **Gli attacchi diventano sempre più costosi.**
Il costo medio causato dall'interruzione delle normali operazioni è aumentato del 26%, da 955.429 $ a 1.207.965 $. Il costo medio causato da danni o furto dei beni e dell'infrastruttura IT è aumentato da 879.582 $ a 1.027.053 $.

3. **L'errore umano è una delle cause principali.**
Delle piccole e medie imprese che hanno subito una violazione dei dati, il 54% ha affermato che la causa principale è stata la negligenza dei dipendenti, aumentata del 48% dallo scorso anno. Tuttavia, come avvenuto nell'anno passato, 1 azienda su 3 fra quelle intervistate per questa ricerca non è riuscita a determinare la causa principale.

4. **Password complesse e autenticazione a più fattori rimangono poco utilizzate.**
Le password continuano a essere una parte integrante della sicurezza informatica. Tuttavia, il 59% degli intervistati ha affermato di non controllare le pratiche dei dipendenti relative alle password, come l'uso di password univoche o complesse e la loro condivisione con altri (nessun cambiamento rispetto all'anno scorso).

> Il 59% afferma di non controllare le pratiche dei dipendenti relative alle password

5. **I malware sono sempre più sofisticati.**
Sempre più aziende sono vittime di exploit e malware che aggirano le protezioni in essere, come i sistemi di rilevamento delle intrusioni (66%, in aumento rispetto al 57%) e le soluzioni antivirus (81% dal 76%).



1—Report: 2017 State of Cybersecurity in Small & Medium-Sized Businesses. Ponemon Institute LLC, 2017

I cinque attacchi più comuni contro le piccole e medie imprese.

1

Phishing/ingegneria sociale

Gli attacchi di ingegneria sociale usano l'interazione umana per ottenere informazioni su un'organizzazione o sui suoi sistemi informatici. Ad esempio, l'hacker può presentarsi come un nuovo dipendente, un addetto alle riparazioni o un ricercatore. Ponendo domande, può essere in grado di raccogliere abbastanza informazioni da infiltrarsi nella rete di un'organizzazione.[2]

Il phishing è una forma di ingegneria sociale. In un attacco di phishing, l'hacker finge di essere un'organizzazione affidabile e usa e-mail o siti Web dannosi per richiedere informazioni personali.[2]

2

Attacchi basati sul Web

Negli attacchi basati sul Web, l'hacker ha accesso a un sito Web legittimo e pubblica malware. Il sito legittimo agisce da host parassita, che infetta gli ignari visitatori. Uno dei tipi più insidiosi di attacchi basati sul Web è il drive-by-download, in cui il contenuto dannoso viene automaticamente scaricato nel computer dell'utente quando naviga nel sito. Non è necessaria alcuna interazione dell'utente.[3]

3

Malware

Malware è un termine ampio che si riferisce a qualsiasi software intenzionalmente progettato per causare danni a un dispositivo o una rete.[4] Include virus, spyware, ransomware e tutti gli altri elementi dannosi con suffisso -ware. Oltre agli attacchi basati sul Web, possono accedere al computer della vittima tramite unità USB o una connessione di rete compromessa.[5]

4

Dispositivi compromessi/rubati

Un dispositivo compromesso o rubato può contenere informazioni preziose e credenziali archiviate localmente che possono consentire un ulteriore accesso alle informazioni e alle reti dell'organizzazione. Password e crittografia dei dati vulnerabili possono ulteriormente aggravare questo tipo di attacco.

5

Attacchi di tipo denial of service

Gli attacchi di tipo denial of service avvengono inondando di traffico la rete bersaglio finché non è più in grado di rispondere o semplicemente si blocca, impedendo l'accesso agli utenti legittimi. Un attacco denial of service distribuito (DDoS) avviene quando più macchine collaborano per attaccare un solo bersaglio, aumentando la potenza dell'attacco. I DDoS incrementano anche la difficoltà di rilevare la reale origine.[6]

2—https://www.us-cert.gov/ncas/tips/ST04-014
3—https://www.symantec.com/content/dam/symantec/docs/security-center/white-papers/web-based-attacks-09-en.pdf
4—https://technet.microsoft.com/en-us/library/dd632948.aspx
5—https://ics-cert.us-cert.gov/sites/default/files/recommended_practices/CaseStudy-002.pdf
6—https://www.us-cert.gov/ncas/tips/ST04-015

Dieci modi per pro-teggersi

Sezione 1:

Attivare l'autenticazione a più fattori

Nomi utente e password sono un obiettivo chiave per gli hacker, per una buona ragione: l'identità è il bene più prezioso. Password complesse e sicure sono molto utili, ma da sole non rappresentano il meccanismo di autenticazione più sicuro. Inoltre, in una realtà di hacking sempre più commercializzato, i ladri non esperti possono esternalizzare il proprio lavoro ad altri. Gli hacker possono acquistare hardware specializzato per scoprire le password, affittare spazi dai fornitori di cloud pubblico o creare un botnet per l'elaborazione.

- Il 90% dei dati rubati tramite phishing è formato da credenziali degli utenti[7]
- L'80-90% delle password può essere violato in meno di 24 ore[8]

L'autenticazione a più fattori (MFA) richiede all'utente di utilizzare due o più credenziali indipendenti per comprovare la propria identità, aumentando notevolmente il livello di sicurezza. Le credenziali possono essere formate da qualcosa che l'utente **conosce** (password o PIN), **possiede** (telefoni Bluetooth® o smart card) o **è** (riconoscimento facciale o delle impronte digitali). Se un fattore risulta compromesso o danneggiato, l'hacker deve comunque fronteggiare un secondo e differente tipo di ostacolo.

L'autenticazione a più fattori di HP e Intel® Authenticate prevedono entrambi la richiesta di vari fattori di autenticazione a ogni tentativo di accesso.

7—Verizon, 2016 Data Breach Investigations Report, 2016
8—Fonte: Brian Contos, CISO di Verodin, Inc. Citato con autorizzazione. https://www.csoonline.com/article/3236716/authentication/how-hackers-crack-passwords and-why-you-cant-stop-them.html

Configurare l'autenticazione a più fattori con HP.

I moderni dispositivi HP Pro o Elite supportano la configurazione della MFA mediante HP Client Security Manager.[9]

1. Aprire Client Security Manager (è necessario accedere come amministratore). Se si apre all'interno di HP Manageability Integration Kit (MIK), è possibile estendere i criteri MFA all'intera flotta di PC.[10]
2. Dal dashboard, fare clic su Standard User Policies (Criteri degli utenti standard).
3. Scegliere i due o tre fattori per i quali si desidera configurare un criterio di accesso e seguire le istruzioni per inserire la credenziale o la coppia di credenziali, come ad esempio la scansione dell'impronta digitale dal lettore di impronte digitali del PC o l'inserimento di un PIN.

Diversificare con Windows Hello.

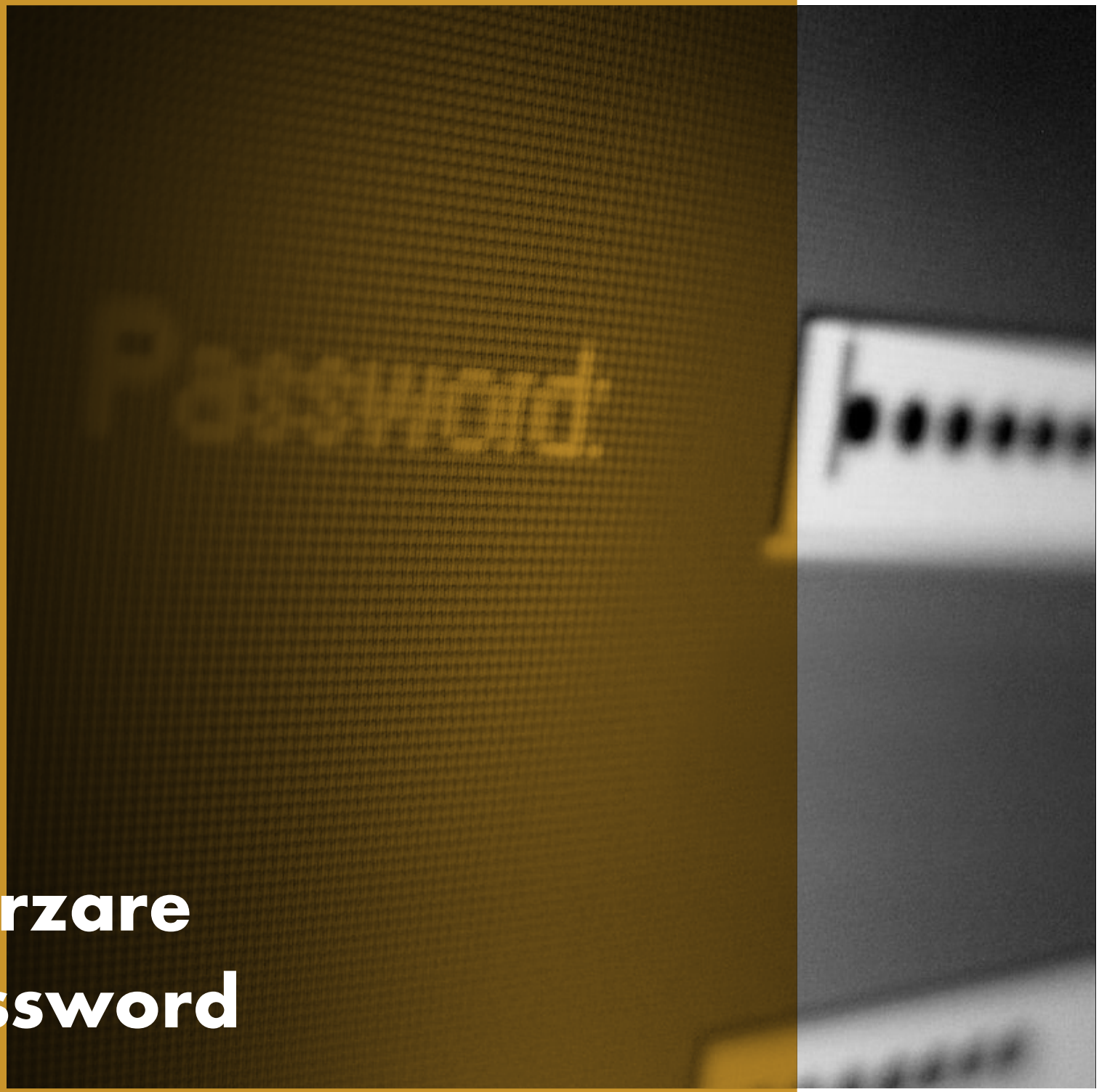
Molti moderni dispositivi Windows 10 Pro con webcam integrata sono compatibili con Windows Hello, compresa l'intera gamma di notebook e convertibili HP. Con la scansione del volto, Windows Hello offre un'alternativa alla password come credenziale MFA.

1. Aprire Impostazioni> Account> Opzioni di accesso
2. In "PIN", selezionare "Aggiungi" se non è già stato configurato.
3. In "Windows Hello", selezionare "Configura" e seguire le istruzioni sullo schermo per eseguire la scansione del volto.

9—HP Client Security Manager Gen4 richiede Windows e processori Intel® o AMD di 8ª generazione.
10—HP Manageability Integration Kit può essere scaricato da http://www.hp.com/go/clientmanagement.

Sezione 2:

Rafforzare le password



Le password sono onnipresenti nella vita di tutti i giorni. Le usiamo praticamente in qualsiasi dispositivo, servizio e account personale o professionale. Poiché rappresentano la prima, e troppo spesso l'unica, linea di difesa per proteggere l'identità e i dati, l'uso di password inefficaci può avere effetti devastanti. Nonostante questo, la maggior parte delle persone non usa password complesse e univoche.

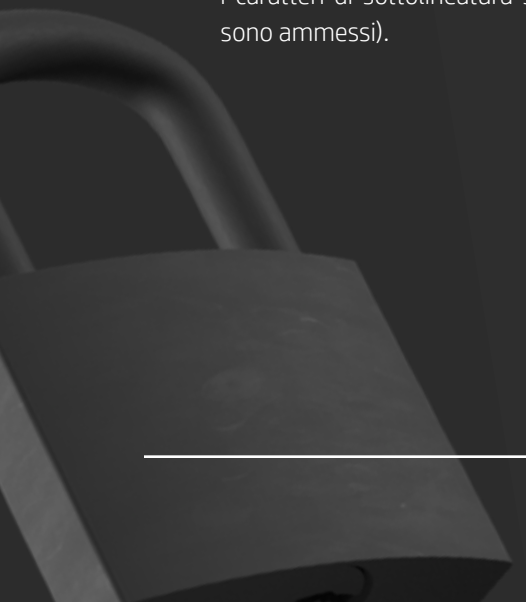
- Il 59% sa che una password sicura è importante, ma solo il 41% ne sceglie una facile da ricordare
- Il 91% comprende i rischi del riutilizzo delle password, ma il 55% le riutilizza comunque
- Solitamente i millennial usano password più complesse rispetto ai baby boomer (65% contro 45%)[11]

Se il proprio dispositivo o servizio non supporta la MFA, la migliore opzione è far lavorare al massimo l'unica password esistente. La maggior parte delle persone non possiede password complesse perché semplicemente non sa come crearle, presupponendo che siano una combinazione casuale di lettere, numeri e simboli. Tuttavia, esistono modi più semplici ed efficaci per aumentare notevolmente il livello di protezione della password.

11—Fonte: LastPass, "New Research: Psychology of Passwords, Neglect is Helping Hackers Win", Katie Petrillo, 1º maggio 2018

Soluzione mnemonica invece che numerica.

Le passphrase mnemoniche sono più sicure delle semplici password e più facili da ricordare rispetto a quelle numeriche.
Se vengono usate al posto delle password semplici, le passphrase mnemoniche sono praticamente impossibili da rubare per gli hacker.



1 Iniziare con una frase facile da ricordare.

Ad esempio, le prime sei parole del Discorso di Gettysburg di Abraham Lincoln, “Four score and 7 years ago”, compongono una passphrase semplice. La citazione rispetta la maggior parte degli standard delle password: tra 8 e 32 caratteri di lunghezza e include lettere maiuscole e minuscole, almeno un numero e un carattere speciale (gli spazi o i caratteri di sottolineatura se gli spazi non sono ammessi).

2 Massimizzare la complessità.

Aumentare la quantità di numeri e caratteri speciali utilizzati. Ad esempio, è possibile modificare le lettere nell’esempio precedente in “4 $core @nd 7 Ye@rs ago”.

3 Personalizzare, non copiare.

È sufficiente allegare un semplice suffisso al termine di ciascuna passphrase per riutilizzare con facilità la password master senza il pericolo di usi duplicati. Per un account Facebook, provare ad aggiungere “FB” al termine della passphrase, o “IG” per Instagram.

Usare uno strumento per la gestione delle password.

Gli strumenti per la gestione delle password sono una delle principali pratiche di sicurezza consigliate dagli esperti. Funzionano generando e memorizzando password lunghe e complicate per ciascun account online, risparmiando all'utente l'obbligo di ricordarle. In generale, sarà sufficiente ricordare una sola password: la password master dello strumento di gestione. La configurazione degli strumenti per la gestione delle password è semplice e il processo è solitamente identico:

1. Scaricare e installare il software e un'estensione per il browser. È anche possibile scaricare un'app per dispositivi mobili.
2. Configurare l'account con l'indirizzo e-mail e la password master.
3. Inserire i dettagli dei vari account.

La maggior parte degli strumenti per la gestione delle password richiede l'aggiornamento manuale delle vecchie password: accedere all'account, andare alle impostazioni e permettere allo strumento per la gestione delle password di generare una password nuova e più sicura. Sostituire le password vecchie e vulnerabili può richiedere tempo, ma aumenta notevolmente la sicurezza.

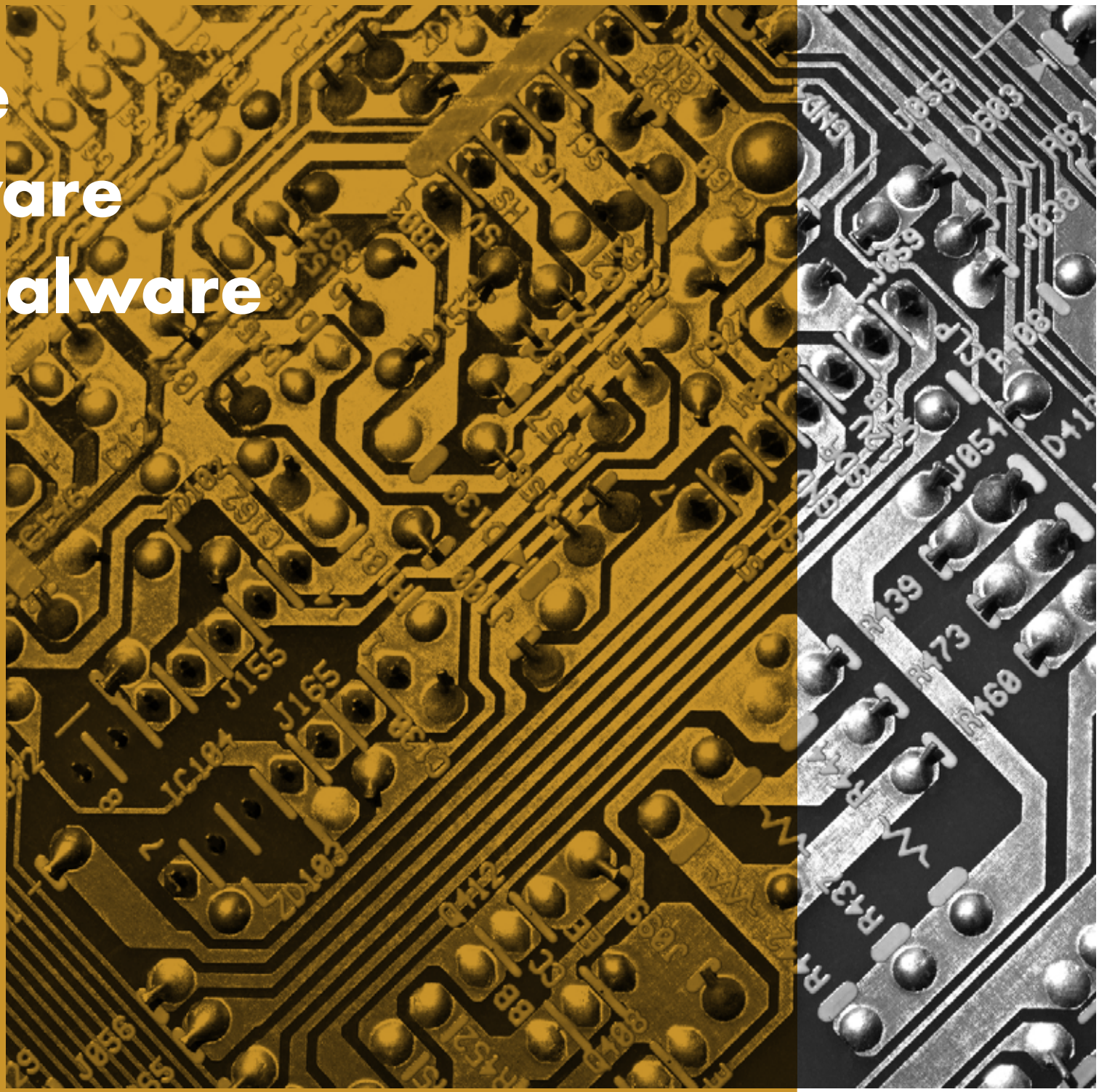
Scegliere uno strumento per la gestione delle password.

Esistono tanti strumenti per la gestione delle password gratuiti, come Bitwarden, Dashlane ed Enpass. In generale, cercare uno strumento per la gestione delle password che:

- Si integri facilmente con il browser più usato
- Consenta di salvare le password in un file crittografato, illeggibile per gli utenti senza la verifica dell'identità. Nello specifico, scegliere uno strumento per la gestione delle password che utilizzi una crittografia AES-256 o più potente.
- Consenta l'autenticazione a due fattori per l'accesso alle password.
- Identifichi un contatto d'emergenza in grado di accedere alle password.
- Memorizzi informazioni di accesso aggiuntive insieme alla password (come domande di sicurezza, numeri di telefono, dettagli dell'account e così via).

Sezione 3:

Usare software antimalware



Senza la protezione dell'antivirus, un PC può venire infettato dai malware entro pochi minuti dalla connessione a Internet.

Malware di ogni tipo possono essere annidati in siti dall'aspetto affidabile o nascosti negli allegati dei messaggi e-mail, e ogni giorno ne vengono creati di nuovi. Il bombardamento dei virus sul PC è costante, quindi lo strumento che lo protegge deve essere forte, ben radicato e regolarmente aggiornato. Un buon programma antimalware soddisfa tutti questi tre requisiti.

In breve, il software antimalware è un programma o un insieme di programmi progettato per prevenire, cercare, rilevare e rimuovere i virus software (e altri software dannosi come worm, trojan, adware e altro). Un tipico programma antimalware esegue regolarmente la scansione del sistema, rimuove automaticamente i malware che trova e avvisa della presenza di download e aggiornamenti software pericolosi.

È necessario possederlo o procurarselo.

Sono molti i prodotti antimalware disponibili. Se nel PC è in esecuzione Windows 10 Pro, l'antivirus Windows Defender è già installato e in esecuzione. In alternativa, è possibile acquistare un programma antimalware di terze parti. Tuttavia, assicurarsi di seguire le istruzioni del fornitore per configurare gli aggiornamenti automatici, in modo da applicare sempre le più recenti protezioni dai virus.

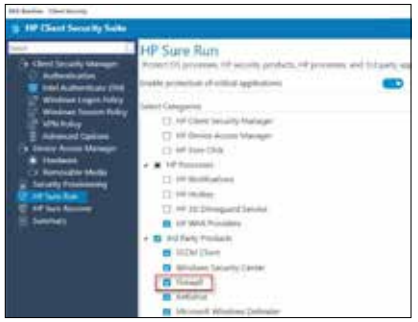
Sempre in esecuzione.

È fondamentale che il software antimalware sia sempre in esecuzione per poter essere efficace. Poiché chi attacca con malware inizia solitamente prendendo di mira i programmi di sicurezza come gli antimalware, questo passaggio non è così semplice come sembra. In Windows 10 Pro è possibile verificare se il programma antivirus è attivo controllando Windows Defender Security Center.

1. Dal menu Start, avviare Windows Defender Security Center e andare su Home.

2. Nell'impostazione "Protezione da virus e minacce", se l'antivirus è in esecuzione viene visualizzato un segno di spunta verde. Se si usa un software antivirus di terze parti, fare clic su "Visualizza provider dell'applicazione antivirus" per visualizzare ulteriori dettagli sullo stato del programma antivirus nel Pannello di controllo di Windows.

Mantenerlo attivo.



I prodotti HP Elite includono anche HP Sure Run[12], un ulteriore livello di sicurezza che garantisce che tutti i processi critici nel PC, compreso il software antivirus, rimangano in esecuzione. Tutti i processi monitorati da Sure Run vengono automaticamente riavviati se disattivati, impedendo che il software antivirus disattivato o bloccato renda l'utente vulnerabile.

HP Sure Run deve essere attivato a livello locale in HP Client Security Manager Gen4.

12—HP Sure Start è disponibile sui prodotti HP Elite dotati di processori Intel® o AMD® di 8ª generazione.

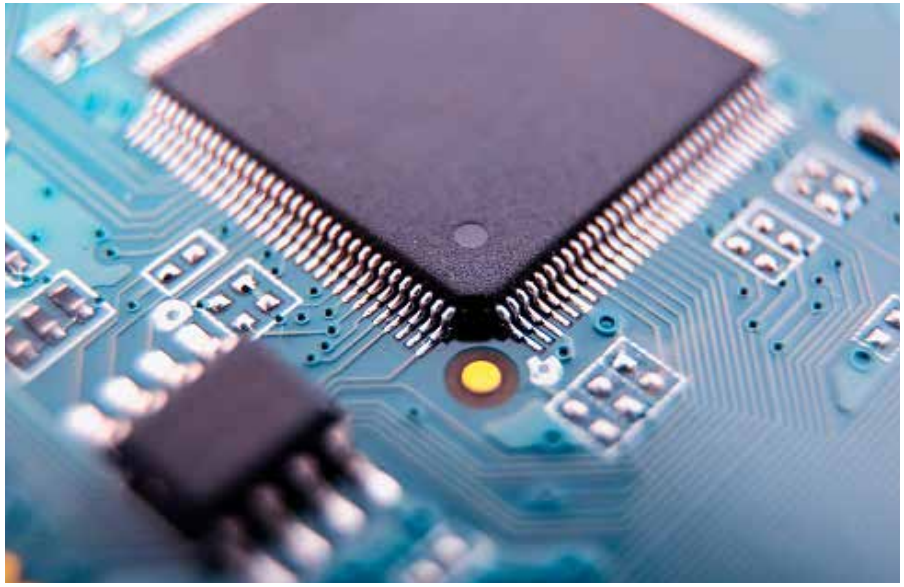
Sezione 4:

Mantenere il software aggiornato

L'antimalware non è l'unico tipo di software che deve affrontare minacce sempre più evolute: è importante tenere aggiornati tutti i software. Se non sono aggiornati, i software potrebbero non disporre di importanti patch di sicurezza contro vulnerabilità scoperte da poco. Questo vale sia per il sistema operativo, ad esempio Windows®, che per tutte le applicazioni in esecuzione sul PC, come i browser Internet, le applicazioni di Office, i software di contabilità, il software antivirus e così via.

L'utente deve anche tenere presente che software obsoleti o fuori produzione potrebbero non ricevere più aggiornamenti di sicurezza. Con il tempo, i criminali informatici trovano le vulnerabilità nei software pubblicati e le sfruttano. Prendendo il sistema operativo come esempio, il controllo della presenza di aggiornamenti in Windows 7 Pro potrebbe non restituire software nuovi, ma in questo modo ignora che Windows 7 Pro non è più la versione più recente di Windows. Applicare la patch a un software meno recente non equivale ad aggiornarlo all'ultima versione: più il software è obsoleto, meno è sicuro.

Più il software è obsoleto, meno è sicuro



Verificare che l'aggiornamento sia applicato.

Man mano che trovano soluzioni alle vulnerabilità, i fornitori di software le pubblicano attraverso gli aggiornamenti software. La maggioranza delle applicazioni dispone di un servizio di aggiornamento integrato nel software, che invia una notifica della disponibilità di un aggiornamento o una patch. Alcuni fornitori software arrivano a installare automaticamente gli aggiornamenti non appena disponibili. Windows 10 Pro, la versione più recente di Windows (quindi la più sicura), dispone di un meccanismo di aggiornamento software automatizzato che mantiene aggiornati il sistema operativo e tutte le altre applicazioni Microsoft, come Microsoft Office.

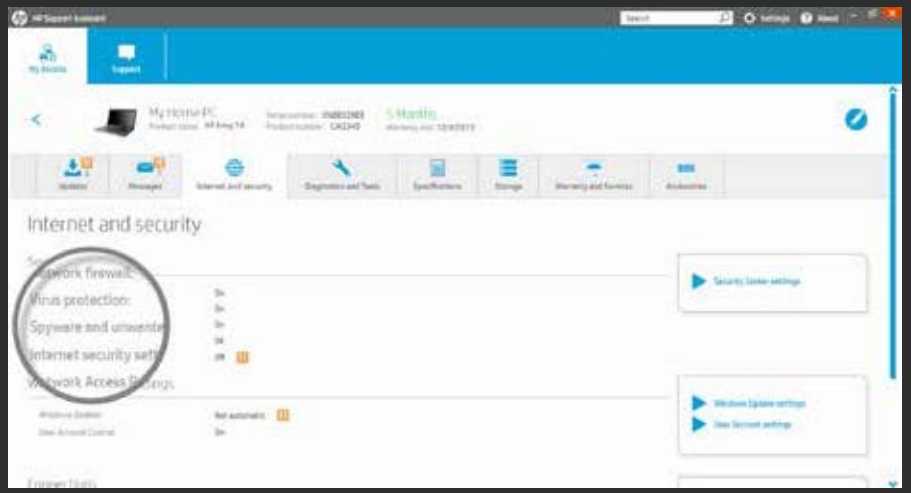
Per verificare se gli aggiornamenti automatici sono attivati:

1. Andare alle impostazioni e scegliere "Aggiornamento e sicurezza".
2. In "Windows Update", scegliere "Opzioni avanzate" e assicurarsi che "Automatico" sia selezionato in "Scegli come installare gli aggiornamenti".
3. Assicurarsi che "Automatico" sia selezionato in "Scegli come installare gli aggiornamenti".

Usare la gestione degli aggiornamenti.

Le dimensioni dei software integrati nel PC possono rendere difficile garantire che *tutto* sia aggiornato. Per questo, molti fornitori di PC offrono strumenti preinstallati che raccolgono automaticamente tutti gli aggiornamenti software e firmware per il sistema. Nei sistemi HP, questo strumento si chiama HP Support Assistant.

Per le applicazioni di terze parti, la funzionalità di aggiornamento viene spesso eseguita da una piccola applicazione di aggiornamento, lanciata al momento dell'avvio. Questi strumenti ausiliari allungano di qualche secondo il tempo di avvio, ma evitano la necessità di cercare gli aggiornamenti nei siti Web dei fornitori delle applicazioni. Se alcuni software non controllano automaticamente la presenza di aggiornamenti o in caso di incertezza, confrontare il numero della versione con il sito Web dello sviluppatore e aggiornare se necessario.



Sezione 5:

Proteggere il browser

I browser, come Internet Explorer o Chrome™, sono il metodo principale con cui accediamo a Internet, pertanto sono il bersaglio principale degli hacker. Solitamente i loro attacchi avvengono per mezzo di un clic accidentale o volontario su un link che lancia un codice dannoso noto come malware.

Alcuni semplici passaggi possono ridurre significativamente le possibilità di un attacco malware attraverso il browser.

Utilizzare un browser protetto.

Internet Explorer, Edge e Chrome offrono tutti potenti funzionalità di sicurezza per Windows. Ad esempio, Edge e Internet Explorer 11 utilizzano Microsoft SmartScreen per eseguire un controllo della reputazione per ogni sito e bloccano quelli che sospettano essere siti di phishing. Inoltre, sui PC HP per uso commerciale, Internet Explorer beneficia dell'ulteriore sicurezza di HP Sure Click: ogni volta che viene aperta una scheda, HP Sure Click la esegue in una macchina virtuale isolata. Questo significa che i codici dannosi rimangono nella scheda e vengono distrutti alla chiusura del browser.[13]

Mantenerlo aggiornato.

Abilitare gli aggiornamenti automatici del browser da Impostazioni. Come già menzionato, tutti gli aggiornamenti della sicurezza saranno applicati al browser, rendendolo molto più sicuro e aumentando la possibilità di fallimento degli attacchi malware.

In Edge, gli aggiornamenti vengono applicati a ogni aggiornamento di Windows. Tuttavia, per controllare se è necessario aggiornare Edge, andare a

- Start
- Impostazioni
- Aggiornamento e sicurezza
- Windows Update
- Verifica presenza di aggiornamenti

13—HP Sure Click è disponibile sulla maggior parte dei PC HP e supporta Microsoft® Internet Explorer e Chromium™. Gli allegati supportati includono i file Microsoft Office (Word, Excel, PowerPoint) e PDF in modalità di sola lettura, se Microsoft Office o Adobe Acrobat sono installati.

Fare attenzione agli avvisi.

La maggior parte dei principali browser moderni dispone di una soglia di base per rilevare i siti Web dannosi e mostrerà un avviso se ritiene che rappresentino una minaccia ragionevole. Alcuni offrono una funzionalità di correzione automatica degli URL, per impedire la navigazione in domini di cui viene comunemente sbagliata l'ortografia (dove spesso vengono ospitati software e siti dannosi).

In Edge, andare a Impostazioni avanzate> Privacy, quindi abilitare le impostazioni "Utilizza un servizio web per risolvere gli errori di navigazione".

Limitare i contenuti e i plug-in.

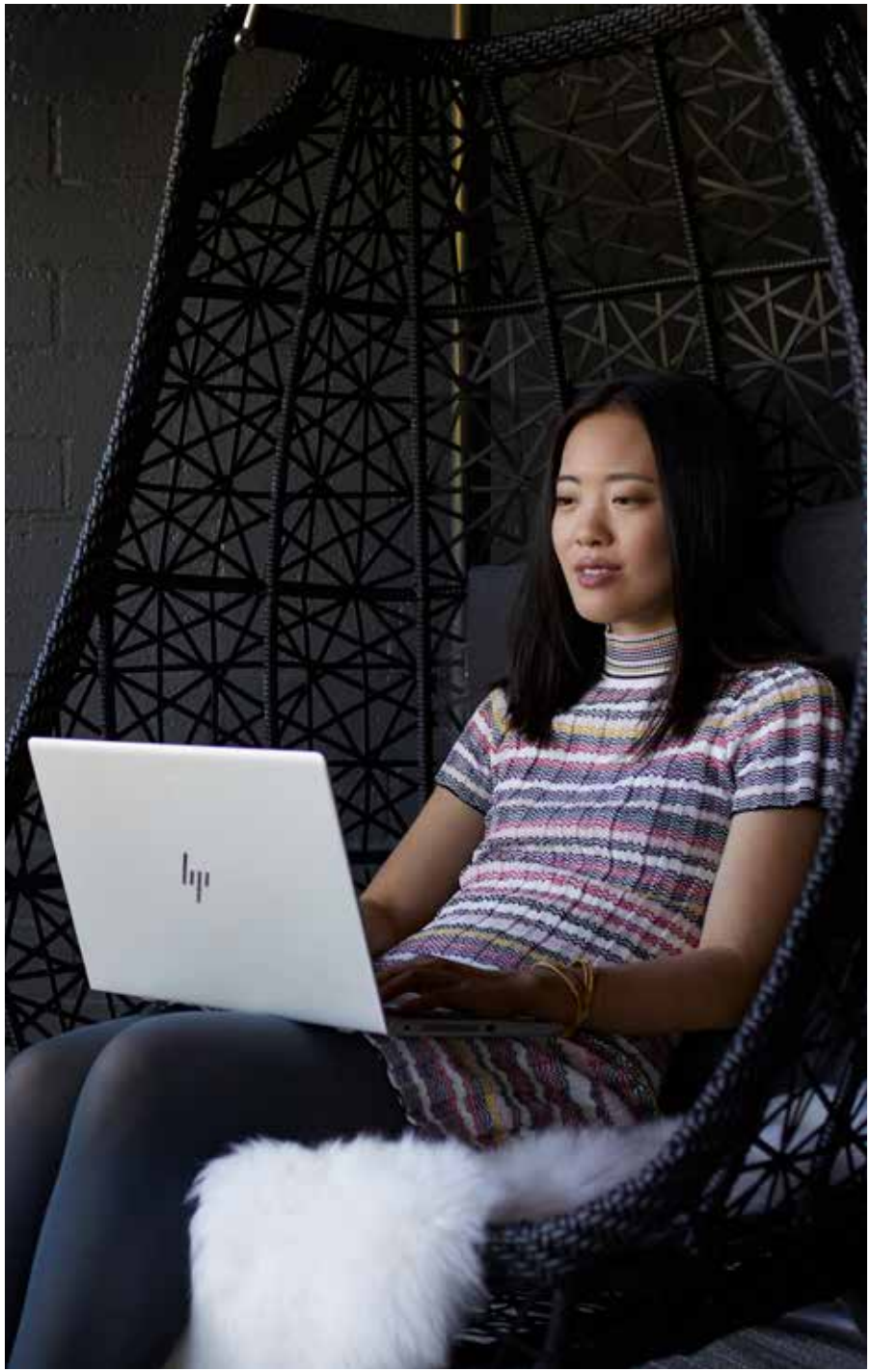
Molti dei componenti aggiuntivi dei browser (come Flash o JavaScript) sono necessari per siti e programmi Web ricchi di contenuti, ma l'incremento dell'accesso al sistema da essi causato rappresenta un punto vulnerabile.

Disattivandoli per impostazione predefinita, un sito deve richiedere l'autorizzazione per il loro uso, garantendo così che solo i siti scelti come affidabili possano utilizzare le loro funzionalità.

In IE, andare a Strumenti (icona dell'ingranaggio)> Opzioni Internet> Sicurezza> Internet> Livello personalizzato...> Esecuzione script. È possibile disattivare JavaScript selezionando semplicemente "Disattiva", oppure fare in modo che venga visualizzata una richiesta di utilizzo selezionando "Chiedi conferma".

Sezione 6:

Sicurezza del router e reti private



Il router è la prima linea di sicurezza dall'intrusione in qualsiasi rete. La connessione a Internet avviene attraverso un router. Questo dispositivo hardware, cablato o wireless (Wi-Fi®), consente la comunicazione tra la rete locale (ad esempio, il PC e altri eventuali dispositivi connessi) e Internet. Per questo, attivare il massimo livello di sicurezza nel router rappresenta il modo migliore per tenere al sicuro PC, stampanti e dati da attacchi dannosi.

> I router sono stati indicati come il tipo di dispositivo più frequentemente bersagliato dagli attacchi IoT.[14]

Poiché trasmettono TUTTI i dati che entrano ed escono dall'abitazione o dall'azienda, comprese le e-mail e le informazioni della carta di credito, i router sono da tempo i bersagli preferiti degli hacker. Nell'Internet Security Threat Report di Symantec del 2018, i router sono stati indicati come il tipo di dispositivo più frequentemente bersagliato dagli attacchi IoT. Gli hacker possono usare malware o difetti di progettazione per nascondere la propria identità, rubare ampiezza di banda, trasformare i dispositivi in zombie botnet o peggio. Possono anche approfittarsi dei dispositivi non protetti.

14—Fonte: Symantec Corporation, 2018 Internet Security Threat Report, 2018

Proteggere la rete.

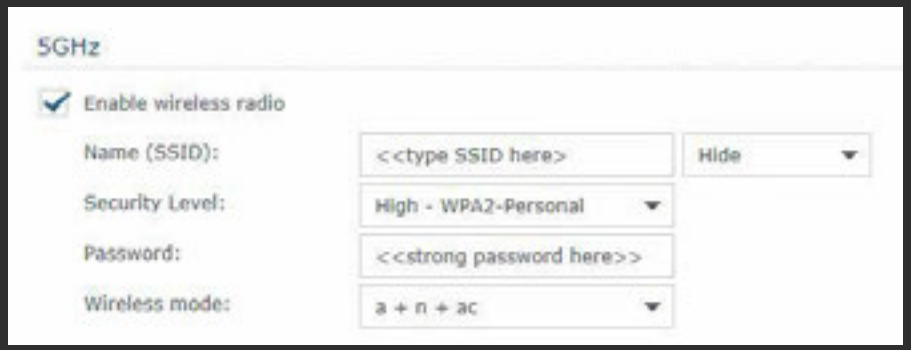
Purtroppo, molti fornitori continuano a offrire configurazioni di router sia protette che non protette. Se un router non è protetto (ovvero, consente le connessioni senza richiedere una password dell'amministratore), tutti possono connettersi al router ed entrare nella rete locale. Un hacker può cambiare le password, spiare o anche accedere ai file su un disco rigido collegato alla rete.

Proteggere sempre il router con password dell'amministratore non predefinite utilizzando i suggerimenti della Sezione 2: Rafforzare le password. Di seguito una schermata che mostra come la maggior parte dei router consenta di impostare le password per proteggerli nella rete.

Configurare la crittografia.

Con i router wireless, le password rappresentano solo una parte della battaglia: scegliere il giusto livello di crittografia è altrettanto importante. La maggior parte dei router wireless supporta quattro protocolli di crittografia wireless: WEP (il più debole), WPA (forte), WPA2 (più forte) e WPA3 (il più forte). Scegliere lo standard di crittografia più forte supportato dal router.

Di seguito una schermata che indica come impostare il livello di crittografia corretto nel router. A questo scopo, è necessario accedere come amministratore del router e navigare fino alle impostazioni di crittografia (variano a seconda del fornitore del router).



Mantenere aggiornato il firmware.

Molti produttori di router pubblicano aggiornamenti software nel corso dell'anno per risolvere i problemi di sicurezza. Come avviene per i software del PC, un router con gli aggiornamenti più recenti è molto meno a rischio di infezione da malware. La maggior parte dei fornitori applica automaticamente gli aggiornamenti del firmware, senza richiedere al cliente di eseguire questa operazione. I modelli di router più recenti possono anche offrire un'app mobile, che è possibile scaricare sul telefono come qualsiasi altra app e utilizzare per verificare la presenza di aggiornamenti. Tuttavia, se il fornitore del router non offre gli aggiornamenti automatici del firmware, è necessario accedere al sito Web del produttore, andare alla sezione relativa all'assistenza e identificare l'aggiornamento corretto in base al modello specifico e all'ID del router (solitamente indicati nel router stesso).

Usare le Virtual Private Network.

Guardando oltre la sicurezza dell'hardware all'interno dell'azienda, una Virtual Private Network (VPN) è un server a cui è possibile connettersi per reindirizzare le attività Internet esterne. Le VPN possono proteggere e mettere al sicuro identità e informazioni. L'obiettivo di una VPN è fornire un metodo principale per navigare nel Web in maniera privata (ma non sempre anonima). Tutto il traffico che passa attraverso la connessione VPN è protetto e, in teoria, non può essere intercettato da nessun altro: questo significa che sono ideali per l'uso sia nelle reti locali che pubbliche. Ulteriori informazioni sulle VPN e sui loro vantaggi sono disponibili nella Sezione 7.

Sezione 7:

Proteggersi nelle reti Wi-Fi® pubbliche

Oggi il Wi-Fi® pubblico è praticamente dovunque. Aeroporti, bar, centri commerciali e addirittura parchi offrono l'accesso gratuito a Internet tramite hotspot. È incredibilmente comodo, e pericoloso.

Gli utenti connessi all'hotspot condividono la stessa rete, quindi esiste una reale possibilità che qualcuno possa approfittare del traffico non protetto. Un hacker può anche configurare un hotspot e tentare di attirare utenti nella sua rete di spoofing (che ha un nome simile). In questo modo può intercettare flussi di dati non crittografati o eseguire attacchi man-in-the-middle per aggirare la crittografia.

È importante presupporre sempre che le proprie comunicazioni siano non protette e pubbliche quando si usa una rete aperta. Tuttavia, senza altre opzioni a disposizione, esistono modi per ridurre l'esposizione.

Limitare la propria attività.
Non trasmettere informazioni altamente sensibili come documenti aziendali, e-mail o password e non utilizzare alcun tipo di applicazione o portale di banking/contabilità.

Creare un piano B.
Se possibile, usare reti semi-aperte che almeno siano protette da password. Solitamente si tratta di reti gestite, che il provider ha interesse a mantenere protette (ad esempio, la sala d'attesa di un aeroporto).

Navigare in siti crittografati.
Assicurarsi di essere connessi a un server Web che supporta il traffico crittografato con il protocollo HTTPS (https://), rispetto al protocollo non protetto in testo normale HTTP. Controllare l'intestazione dell'URL di un sito: un browser moderno solitamente dispone di un'icona nella barra dell'URL che indica la presenza di HTTPS e la validità del certificato (spesso mediante l'icona di un lucchetto o il colore verde). Facendo clic sull'area viene visualizzata una finestra di dialogo che descrive ulteriormente il livello di crittografia.

Reindirizzare tutto il traffico con una VPN.
Come menzionato nella sezione precedente, una VPN è in grado di proteggere i dati quando la connessione di rete non è affidabile: una rete Wi-Fi® pubblica è un esempio perfetto. Un tunnel VPN esegue la crittografia end-to-end dei dati, assicurando che un potenziale intercettatore non sia in grado di interpretare l'attività. Non tutte le VPN sono uguali, quindi è necessario scegliere quella giusta in base al budget e al tipo di dispositivo. Le VPN gratuite hanno spesso una larghezza di banda limitata e protocolli di crittografia semplici, quindi la velocità di navigazione sarà inferiore e si potrebbe comunque essere esposti a rischi. Detto ciò, una VPN gratuita affidabile è probabilmente una soluzione migliore rispetto a nessuna VPN.

Sezione 8:

Fermare gli hacker visivi

L'hacking visivo avviene quando informazioni sensibili vengono visualizzate su schermi in luoghi pubblici e competitor, ladri di identità o individui senza scrupoli li vedono, acquisiscono e sfruttano. Anche il passante curioso rappresenta una potenziale minaccia. Tutto è a rischio, dalle password, ai numeri del conto, ai dati finanziari, alle informazioni proprietarie dell'azienda, e nessun software di sicurezza è in grado di impedire a queste persone di dare un'occhiata.

Man mano che il moderno ambiente di lavoro si allontana sempre di più dagli uffici tradizionali a spazi pubblici e remoti, la possibilità di subire un hacking visivo è sempre più reale. Infatti, oggi l'hacking visivo rappresenta per le aziende una delle minacce low-tech più sottovalutate. È semplice, efficace e spesso non viene notato finché non è troppo tardi.

Secondo una ricerca pubblicata dal Ponemon Institute[1]:

- Il 91% dei tentativi di hacking visivo è riuscito
- Il 68% dei tentativi di hacking visivo non è stato notato dalla vittima
- Il 52% delle informazioni sensibili è stato rubato direttamente dagli schermi dei dispositivi

Prestare attenzione al proprio ambiente.

Quando si lavora in spazi pubblici, presupporre sempre che qualcuno stia sbirciando da dietro le spalle e scegliere le attività di conseguenza.

Limitare la propria esposizione.

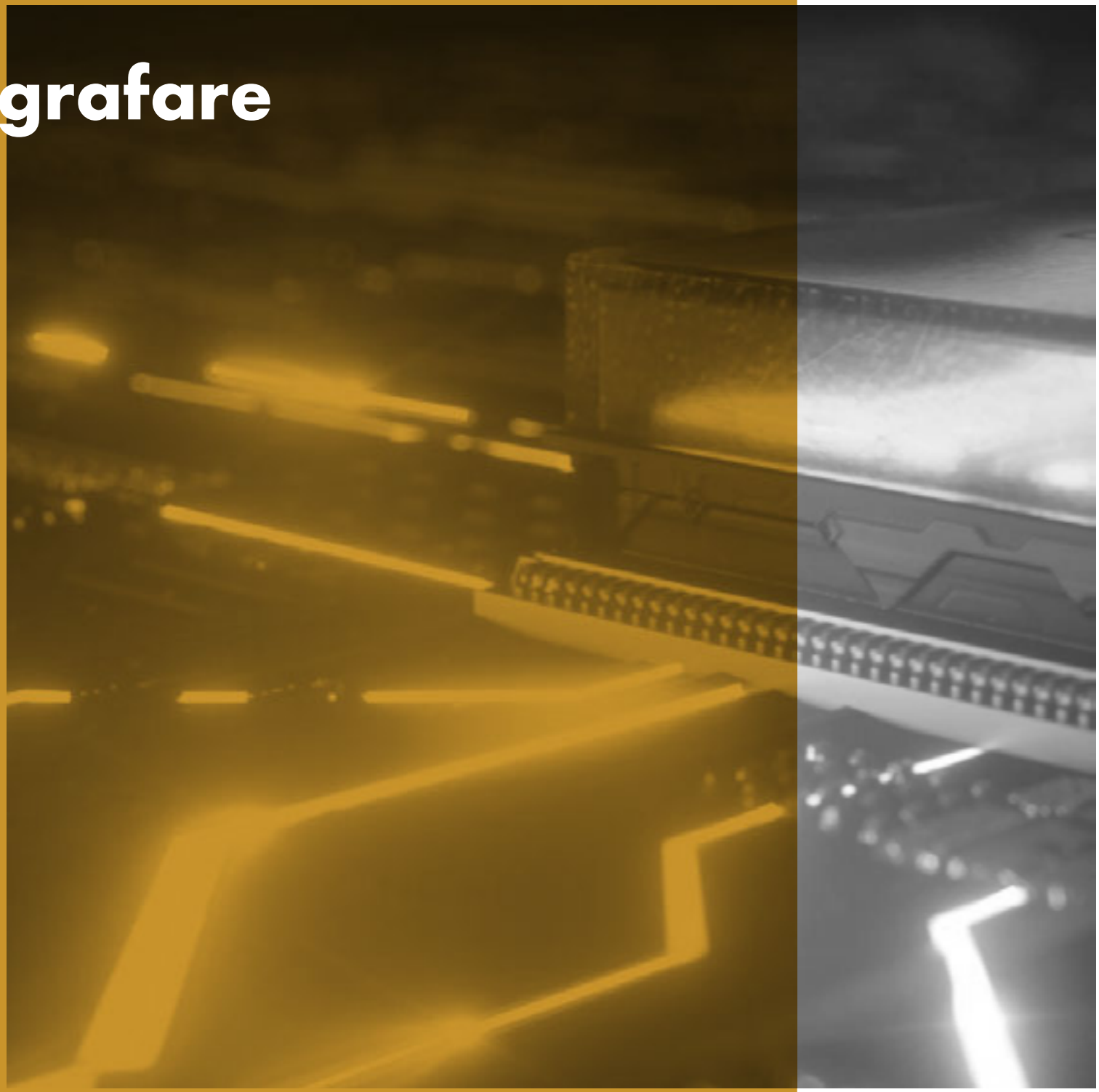
Gli schermi per la privacy sono progettati per ridurre gli angoli di visualizzazione delle schermate, in modo che il potenziale hacker visivo non riesca a vedere ciò che viene visualizzato se non si trova direttamente davanti. Un filtro esterno è un metodo semplice per aggiungere questo tipo di sicurezza. Si attacca allo schermo e può essere rimosso quando è necessario condividere la schermata con un pubblico più vasto.

In alternativa, uno schermo per la privacy integrato semplifica questo processo, evitando l'obbligo di applicare, riporre e riposizionare una protezione esterna. Molti PC HP offrono come optional HP Sure View Gen2[15], uno schermo per la privacy integrato progettato per scoraggiare l'hacking visivo. Modifica dinamicamente la struttura dei pixel LCD a livello molecolare, consentendo di attivarli e disattivarli con un tasto e migliorando le prestazioni sia in ambienti luminosi che oscuri.

15—Lo schermo per la privacy HP Sure View integrato è una caratteristica opzionale che deve essere configurata al momento dell'acquisto ed è progettata per funzionare con orientamento orizzontale.

Sezione 9:

Crittografare i dati



Quando un PC viene smarrito o rubato, il disco rigido è il primo bersaglio dell'attacco. Solo poche viti lo tengono in posizione e, una volta rimosso, può essere collegato a un altro PC. Se i dati non sono stati correttamente protetti, leggere un disco è come spalancare un libro.

La crittografia garantisce che i dati all'interno rimangano completamente illeggibili. La crittografia è il processo di codifica dei dati che li rende illeggibili da chiunque non disponga della chiave di crittografia segreta. Quindi, un computer con un disco rigido crittografato può essere rubato ma non letto: è un risultato di gran lunga migliore rispetto alle informazioni aziendali o personali nelle mani sbagliate, per sempre.

Attivare la crittografia software.

Windows 10 Pro supporta la crittografia delle password del disco rigido usando le credenziali di accesso come chiave. In questo modo, l'hacker ha bisogno del nome utente e della password per accedere ai dati.

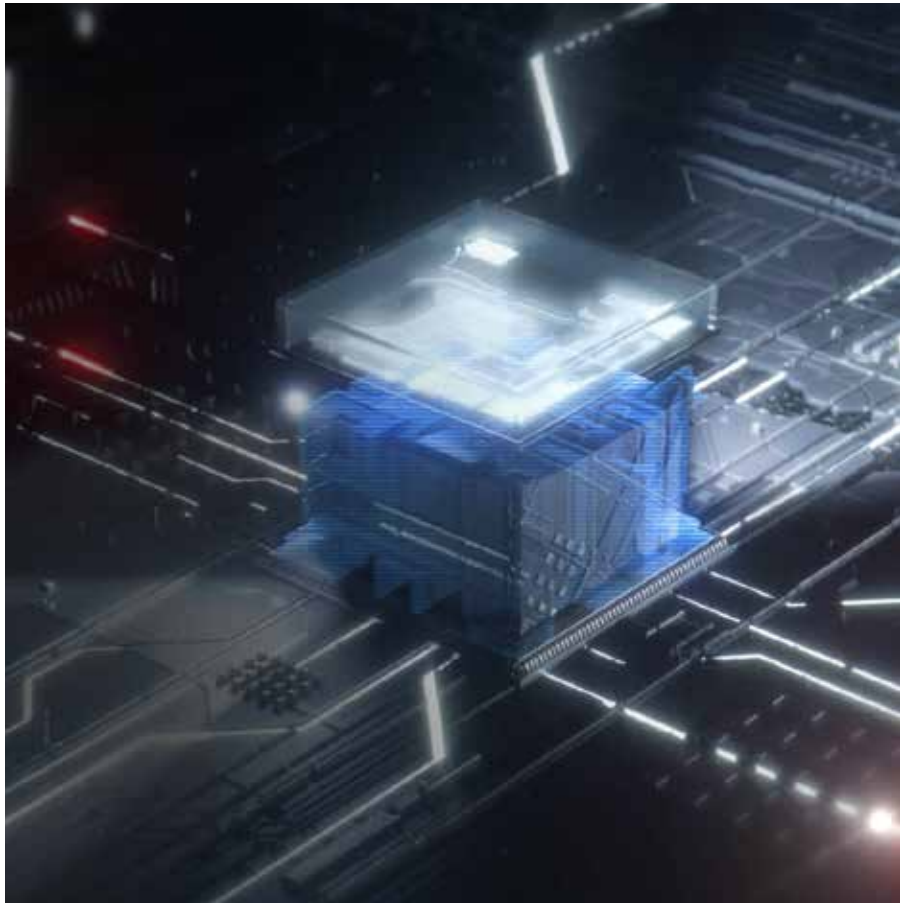
1. Assicurarsi di disporre di una password complessa per l'account utente:
   - Impostazioni> Account> Opzioni di accesso> Password

2. Se disponibile, attivare Trusted Platform Module (TPM), che attiva un chip di sicurezza all'interno del PC per crittografare le nuove password e i dati sul disco:
   - Impostazioni> Aggiornamento e sicurezza> Sicurezza di Windows> Sicurezza dispositivi> Processore

3. Attivare Crittografia, che garantisce che i dati non possano essere visti o copiati senza le credenziali:
   - Impostazioni> Aggiornamento e sicurezza> Crittografia unità

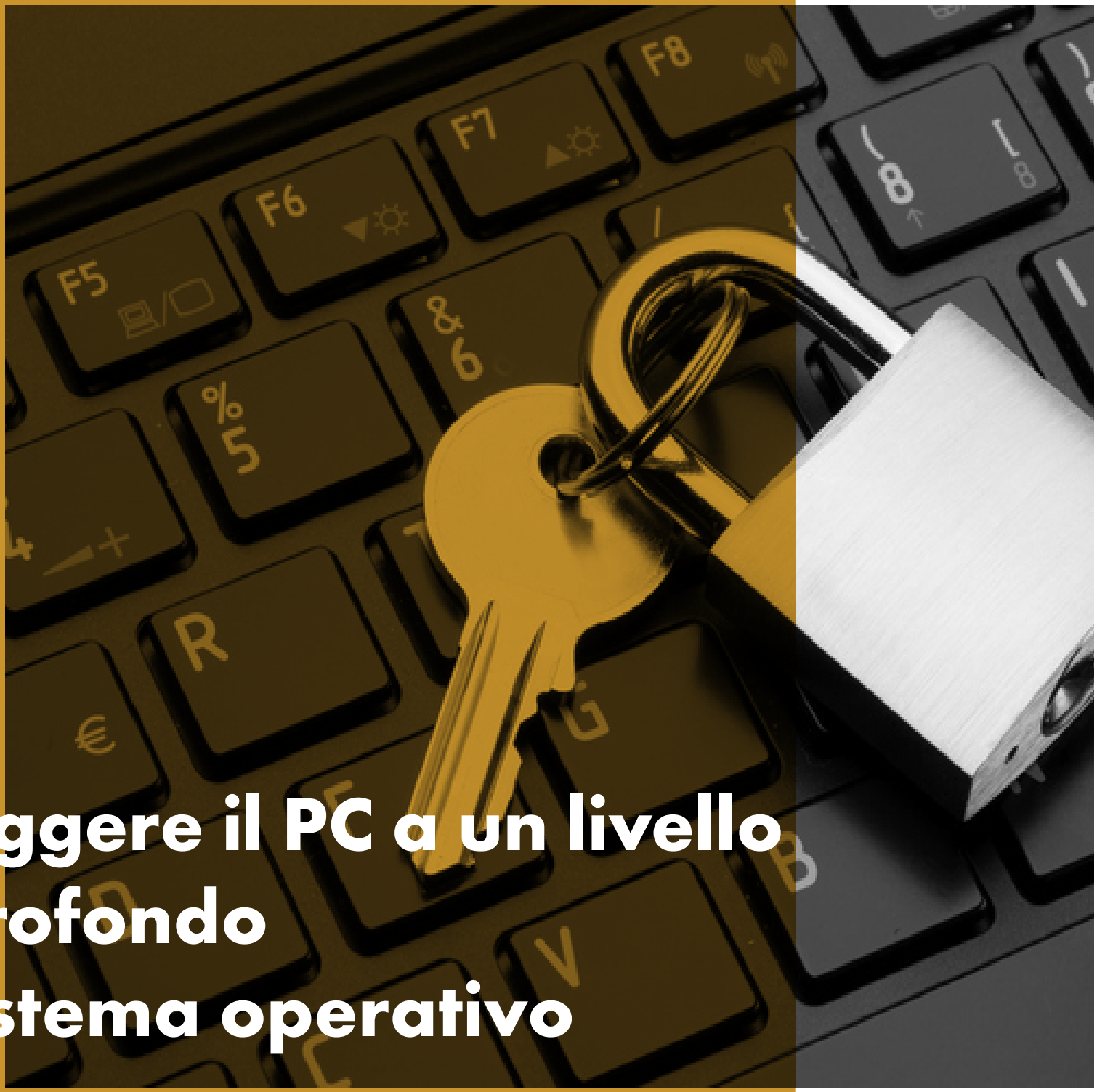
Sfruttare la crittografia hardware.

BitLocker è una funzionalità di Windows 10 Pro che fornisce crittografia software, sbloccata mediante una chiave hardware. I dispositivi con chip TPM, come i notebook HP, sono in grado di crittografare senza hardware extra. TPM impedisce l'accesso ai dati crittografati se rileva che il sistema è stato manomesso da spento. Anche i dispositivi senza TPM possono utilizzare BitLocker, ma richiedono un dispositivo mobile, come un'unità USB, che funzioni da chiave.



Sezione 10:

Proteggere il PC a un livello più profondo del sistema operativo



Il BIOS (Basic Input Output Software) è il software che avvia il computer e che carica il sistema operativo. Se infettano questo software di base, le spie possono installare un malware che rimane attivo e non viene rilevato dagli antivirus. Rimane anche se viene cancellato il disco rigido o se viene reinstallato il sistema operativo.

Se riesce ad accedere al BIOS, un hacker riesce essenzialmente a controllare qualsiasi aspetto del PC.

In questo modo riesce a estrarre i dati o danneggiare il sistema modificando il firmware, cosa che richiede la sostituzione dell'intero sistema, che deve essere riparato.
Per i PC HP Elite e Pro, HP Sure Start è in grado di curare automaticamente il BIOS da malware, rootkit o danni, aggiungendo un ulteriore livello di protezione e creando una base affidabile per la sicurezza del PC.[16]

Non ignorare alcun aggiornamento.

Come menzionato nella Sezione 4, gli aggiornamenti software garantiscono che le nuove vulnerabilità scoperte vengano risolte, e il BIOS non fa eccezione. Poiché nella forza lavoro o in una base di utenti la maggior parte delle implementazioni del BIOS condivide lo stesso codice sorgente, le vulnerabilità rilevate sono probabilmente presenti in molte implementazioni del fornitore di PC. Strumenti OEM come HP Support Assistant controllano automaticamente la presenza di aggiornamenti; altrimenti, è possibile controllare nel sito del produttore la presenza di aggiornamenti del BIOS.

Esaminare il BIOS.

Le impostazioni di fabbrica del BIOS possono essere considerate il giusto equilibrio tra sicurezza e usabilità. Tuttavia, per proteggere il sistema dai tanti possibili metodi di trasferimento di codici dannosi, si consiglia di rimuovere alcune delle sue funzionalità.

La modalità di accesso al BIOS può variare leggermente a seconda del produttore, ma solitamente avviene premendo un tasto funzione all'avvio iniziale (F10 o FN-10 sui notebook HP).

16—HP Sure Start Gen4 è disponibile sui prodotti HP Elite e HP Pro 600 dotati di processori Intel® o AMD di 8ª generazione.

Impostare una password del BIOS.

Per proteggere le impostazioni del BIOS dalla modifica da parte di utenti non autorizzati, si consiglia di impostare una password:

- Ad esempio: Security> Administrator Tools> Create BIOS Administrator Password

È importante ricordare la password del BIOS, in quanto è progettata per non essere aggirata o recuperata.

Impostare una password all'accensione.

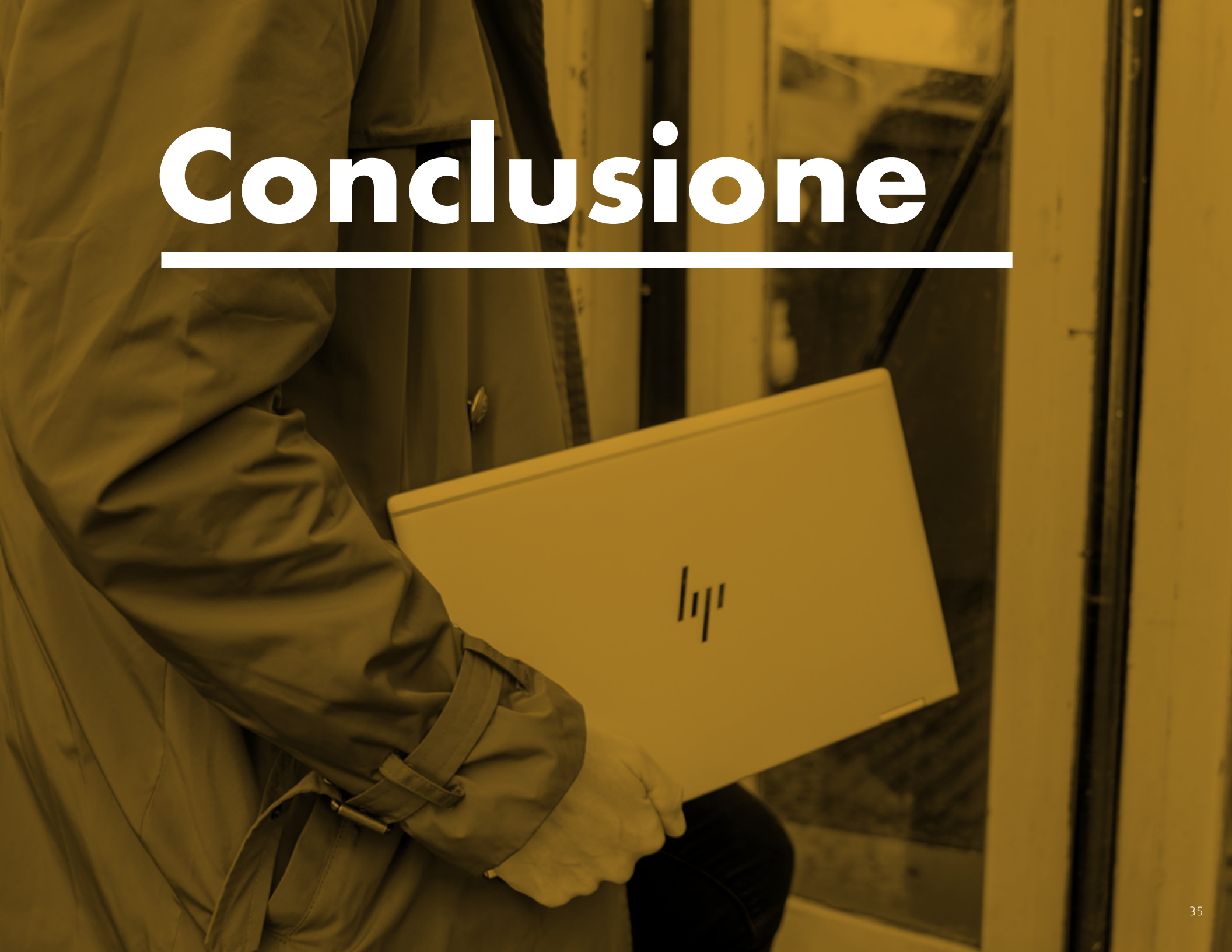
Per una sicurezza ancora maggiore, è possibile creare una password all'accensione. Ogni volta che viene acceso il PC, prima che il sistema esegua qualsiasi programma, viene richiesta questa password. Come la password del BIOS, è difficile da recuperare o ripristinare e dimenticarla rende il computer inutilizzabile.

Limitare le funzionalità non utilizzate.

Nel BIOS è necessario valutare alcune impostazioni per ottenere la massima sicurezza. Anche se rimuovono alcune funzionalità o riducono l'accessibilità, attivano una sicurezza a un livello più basso rispetto al sistema operativo che non è possibile replicare con i software:

1. Rimuovere i dispositivi esterni e ottici dall'ordine di avvio (Es: Advanced> Boot Options). In particolare, questo riguarda l'avvio da unità USB, da rete (PXE) e da unità ottica, in quanto consentono di caricare i malware da fonti esterne. Se è necessario avviare da questi dispositivi, questa funzionalità può essere attivata caso per caso.
2. Disattivare il supporto legacy (Es: Advanced> Secure Boot Configuration) e attivare l'avvio sicuro.
3. Attivare la funzionalità "Save/Restore GPT of System Hard Drive" (Es: Security> Hard Drive Utilities).
4. Attivare DriveLock e impostare una password.

Conclusione



Oggi le minacce digitali sono più che mai rivolte alle piccole e medie imprese. La buona notizia è che gran parte dell'hardware e software utilizzato contiene funzionalità di sicurezza poco usate in grado di combatterle. Inoltre, è disponibile un numero senza precedenti di prodotti e servizi con innovazioni all'avanguardia sulla sicurezza, in grado di proteggere dalle minacce sconosciute di domani. Dalla sicurezza basata sull'hardware nei dispositivi attuali all'aggiornamento automatico del software, un investimento intelligente su dispositivi sicuri e connessi ripagherà nel lungo termine. HP progetta soluzioni per la sicurezza che fanno leva sui punti di forza di Windows 10 Pro, sfruttando le funzionalità di sicurezza integrate con incrementi hardware discreti e assistenza software sempre aggiornata. Le minacce da affrontare cambiano ogni giorno e la strategia di sicurezza giusta aumenta notevolmente le possibilità di combatterle.

GRAZIE

Per ulteriori informazioni, visitare:
http://www8.hp.com/it/it/elite-family/windows10/index.html

+ Windows 10

Più protezione, dall'accensione allo spegnimento.