Windows 10 Pro

DAS PRAXIS-HANDBUCH ZUR CYBER-SICHERHEIT

Zehn Maßnahmen, die jedes Unternehmen ergreifen sollte, um sich gegen Cyberangriffe zu schützen.

Sorgen Sie für einen besseren Rund-um-Schutz.

Die Landschaft der Cybersicherheit ändert und erweitert sich ständig. Kleine und mittelständische Unternehmen sehen sich zunehmend Cyberangriffen ausgesetzt, die ihre Informationen bedrohen – und die personenbezogenen Daten ihrer Kunden. Dieses Handbuch wurde konzipiert, um diesen kleinen und mittelständischen Unternehmen mit begrenzten IT-Ressourcen dabei zu helfen, ihre Cybersicherheit noch heute zu stärken. Und das sogar kostenlos oder zumindest kostengünstig.

INHALTSVERZEICHNIS

I.

Die Bedrohungslandschaft

Die Cybersicherheitstrends kleiner und mittelständischer Unternehmen

Die fünf häufigsten Angriffe gegen kleine und mittelständische Unternehmen

II.

Zehn Wege, wie Sie sich schützen können

1. Aktivieren Sie die mehrstufige Authentifizierung
2. Stärken Sie Ihre Passwörter
3. Verwenden Sie Anti-Malware-Software
4. Halten Sie Ihre Software auf dem neuesten Stand
5. Sichern Sie Ihren Browser
6. Sichern Sie Ihr Netzwerk
7. Schützen Sie sich im öffentlichen WLAN®
8. Stoppen Sie visuelle Hacker
9. Verschlüsseln Sie Ihre Daten
10. Sichern Sie Ihren PC unterhalb der Betriebssystemebene

III.

Fazit

© Copyright 2018 HP Development Company, L.P.

Die Bedrohungs-landschaft

Die Cyber-sicherheitstrends kleiner und mittelständischer Unternehmen

Dies sind laut dem Ponemon Institute[1] fünf der Top-Trends kleiner und mittelständischer Unternehmen im Bereich Cybersicherheit:

1. **Immer mehr Unternehmen sehen sich Angriffen ausgesetzt.**
In den vergangenen 12 Monaten stieg der Prozentsatz der angegriffenen Unternehmen um 11 %, von 55 Prozent auf 61 Prozent. Die häufigsten Angriffe auf kleinere Unternehmen erfolgen mithilfe von Phishing/Social Engineering (48 %) oder sind webbasiert (43 %). Gleichzeitig werden die Cyberangriffe zunehmend gezielter, schwerwiegender und ausgefeilter.

2. **Das macht sie kostspieliger.**
Die durchschnittlichen Kosten für die Unterbrechung des normalen Betriebs stiegen um 26 %, von 955.429 US-Dollar auf 1.207.965 US-Dollar. Die durchschnittlichen Kosten, die aufgrund von Beschädigung oder Diebstahl von IT-Ressourcen oder -Infrastrukturen entstanden, stiegen von 879.582 US-Dollar auf 1.027.053 US-Dollar.

3. **Eine der Hauptursachen sind menschliche Fehler.**
54 % der kleinen oder mittelständischen Unternehmen, die Datenschutzverletzungen erlitten, gaben als Hauptgrund die Nachlässigkeit von Mitarbeitern an – im Vergleich zum Vorjahr ist dies ein Anstieg von 48 %. Allerdings konnte ebenso wie im letzten Jahr nur eines von drei Unternehmen, die an dieser Recherche teilgenommen hatten, die Grundursache nennen.

4. **Starke Passwörter und die Multi-Faktor-Authentifizierung werden nach wie vor nicht ausreichend genutzt.**
Passwörter bilden immer noch einen wesentlichen Teil der Cybersicherheit. Dennoch gaben 59 % der Befragten an, sie hätten keinen Einblick in die Passwort-Praktiken ihrer Angestellten. So wüssten sie beispielsweise nicht, ob einzigartige oder starke Passwörter verwendet oder Passwörtern an Dritte weitergegeben würden – auch hier hat sich im Vergleich zum Vorjahr nichts geändert.

> 59 % geben an, sie hätten keinerlei Einblick in die Passwort-Praktiken ihrer Angestellten

5. **Malware wird immer ausgefeilter.**
Immer mehr Unternehmen werden Opfer von Exploits oder Malware, die ihre bestehenden Schutzmaßnahmen wie Angriffserkennungssysteme (von 57 % auf 66 % gestiegen) und Virenschutzlösungen (von 76 % auf 81 % gestiegen) umgehen.

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

Die fünf häufigsten Angriffe gegen kleine und mittelständische Unternehmen.

1

Phishing/Social Engineering

Angriffe durch Social Engineering nutzen zwischenmenschliche Interaktionen, um Informationen über eine Organisation oder deren Computersysteme in Erfahrung zu bringen. Zu diesem Zweck gibt sich der Hacker beispielsweise als neuer Mitarbeiter, als Servicetechniker oder als Forscher aus. Durch das Stellen von Fragen kann er oder sie dann möglicherweise genug Informationen erfassen, um das Netzwerk einer Organisation zu infiltrieren.[2]

Phishing ist eine Form des Social Engineering. Bei einer Phishing-Attacke gibt sich der Angreifer als vertrauenswürdige Organisation aus und verwendet E-Mails oder betrügerische Websites, um an personenbezogene Daten zu gelangen.[2]

2

Webbasierte Angriffe

Im Falle von webbasierten Angriffen erlangt der Angreifer Zugriff auf eine legitime Website und postet auf dieser Malware. Die eigentlich legitime Website agiert so als parasitärer Host, der ahnungslose Besucher infiziert. Zu den heimtückischsten Arten webbasierter Angriffe zählt der „Drive-by-Download", bei dem automatisch schädliche Inhalte auf den Computer eines Benutzers heruntergeladen werden, sobald dieser die Website besucht. Hierzu ist keinerlei Benutzerinteraktion erforderlich.[3]

3

Malware

Malware ist ein Sammelbegriff, der sich auf sämtliche Software bezieht, die dazu konzipiert wurde, einem Gerät oder einem Netzwerk zu schaden.[4] Hierzu zählen Viren, Spyware, Ransomware und all die anderen „-ware". Malware kann nicht nur über das Internet, sondern auch über einen USB-Stick oder eine kompromittierte Netzwerkverbindung auf den Computer eines Opfers gelangen.[5]

4

Kompromittierte/gestohlene Geräte

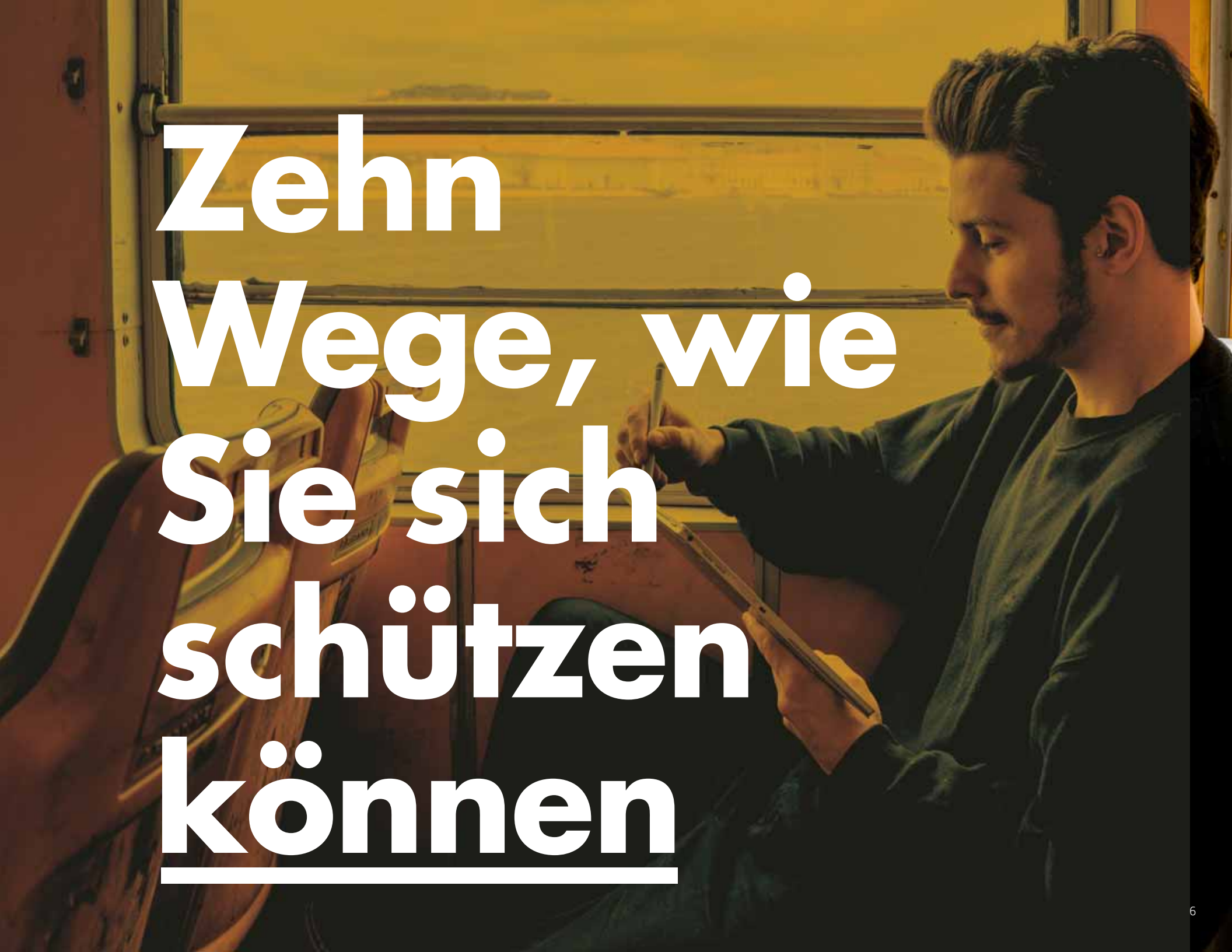
Ein Gerät, das kompromittiert oder gestohlen wurde, kann wertvolle Daten und lokal gespeicherte Anmeldeinformationen enthalten, die den Zugriff auf die Daten und das Netzwerk des Unternehmens ermöglichen können. Schwache Passwörter und eine unzureichende Datenverschlüsselung können diese Art des Angriffs noch verschlimmern.

5

Denial-of-Service-Angriffe

Denial-of-Service-Angriffe erfolgen, indem das Zielnetzwerk mit Datenverkehr überflutet wird, bis dieses nicht mehr antworten kann oder einfach zusammenbricht, sodass legitime Benutzer es nicht mehr nutzen können. Distributed-Denial-of-Service-Angriffe (verteilte Dienstverweigerungsangriffe) (DDoS) erfolgen, wenn mehrere Maschinen zusammenarbeiten, um ein einziges Ziel anzugreifen, wodurch die Wirkung des Angriffs maßgeblich verstärkt wird. DDoS machen es zudem schwierig, die wahre Quelle ausfindig zu machen.[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



Zehn Wege, wie Sie sich schützen können

Abschnitt 1:

Aktivieren Sie die mehrstufige Authentifizierung

Benutzernamen und Passwörter zählen zu den zentralen Zielen der Hacker und das aus gutem Grund – Ihre Identität ist die wertvollste Ressource. Starke und sichere Passwörter sind sehr effektiv, aber Passwörter allein stellen nicht gerade den sichersten Authentifizierungsmechanismus dar. Und in einer Welt des zunehmend auch kommerzialisierten Hacking können weniger erfahrene Diebe diese Arbeit ohne Weiteres von anderen erledigen lassen. Heutzutage können Hacker speziell für das Knacken von Passwörtern konzipierte Hardware erwerben, Speicherplatz bei öffentlichen Cloud-Anbietern mieten oder für die Bearbeitung ein Botnet erstellen.

- 90 % der gestohlenen Daten sind Anmeldeinformationen von Benutzern[7]
- 80–90 % der Passwörter können in weniger als 24 Stunden geknackt werden[8]

Bei der Multi-Faktor-Authentifizierung müssen Sie zwei oder mehr unabhängige Anmeldedaten verwenden, um Ihre Identität nachzuweisen, wodurch Ihr Sicherheitsniveau entschieden erhöht wird. Anmeldedaten können etwas sein, das dem Benutzer **bekannt** ist (Passwörter oder PINs), etwas, das der Benutzer **besitzt** (Bluetooth®-Telefone oder Smartcards) oder etwas, das der Benutzer **ist** (Gesichts- oder Fingerabdruckerkennung). Wenn ein Faktor kompromittiert oder geknackt wird, sieht sich der Angreifer noch einem zweiten, anderen Hindernis gegenüber.

HP MFA und Intel® Authenticate unterstützen mehrere Authentifizierungsfaktoren, die bei jedem Login-Versuch erforderlich sind.

7) Verizon, 2016 Data Breach Investigations Report, 2016
8) Source: Brian Contos, CISO at Verodin, Inc. Quoted with permission. https://www.csoonline.com/article/3236716/authentication/how-hackers-crack-passwords and-why-you-cant-stop-them.html

Richten Sie die mehrstufige Authentifizierung in HP ein.

Moderne HP Pro- oder Elite-Geräte unterstützen die Einrichtung der mehrstufigen Authentifizierung mit dem HP Client Security Manager.[9]

1. Öffnen Sie den Client Security Manager (Sie müssen als Administrator angemeldet sein, um das tun zu können). Wenn Sie den Manager innerhalb des Manageability Integration Kit (MIK) von HP öffnen, können Sie Ihre MFA-Strategien auf Ihre gesamte PC-Flotte übertragen.[10]
2. Klicken Sie im Dashboard auf „Standardmäßige Benutzerstrategien“.
3. Wählen Sie die zwei oder drei Faktoren, für die Sie eine Login-Strategie festlegen möchten, und befolgen Sie die genannten Anweisungen, um die Anmeldedaten zu registrieren – beispielsweise durch das Scannen Ihres Fingerabdrucks auf dem Fingerabdruckleser des PCs oder durch das Eingeben einer PIN.

Variieren Sie mit Windows Hello.

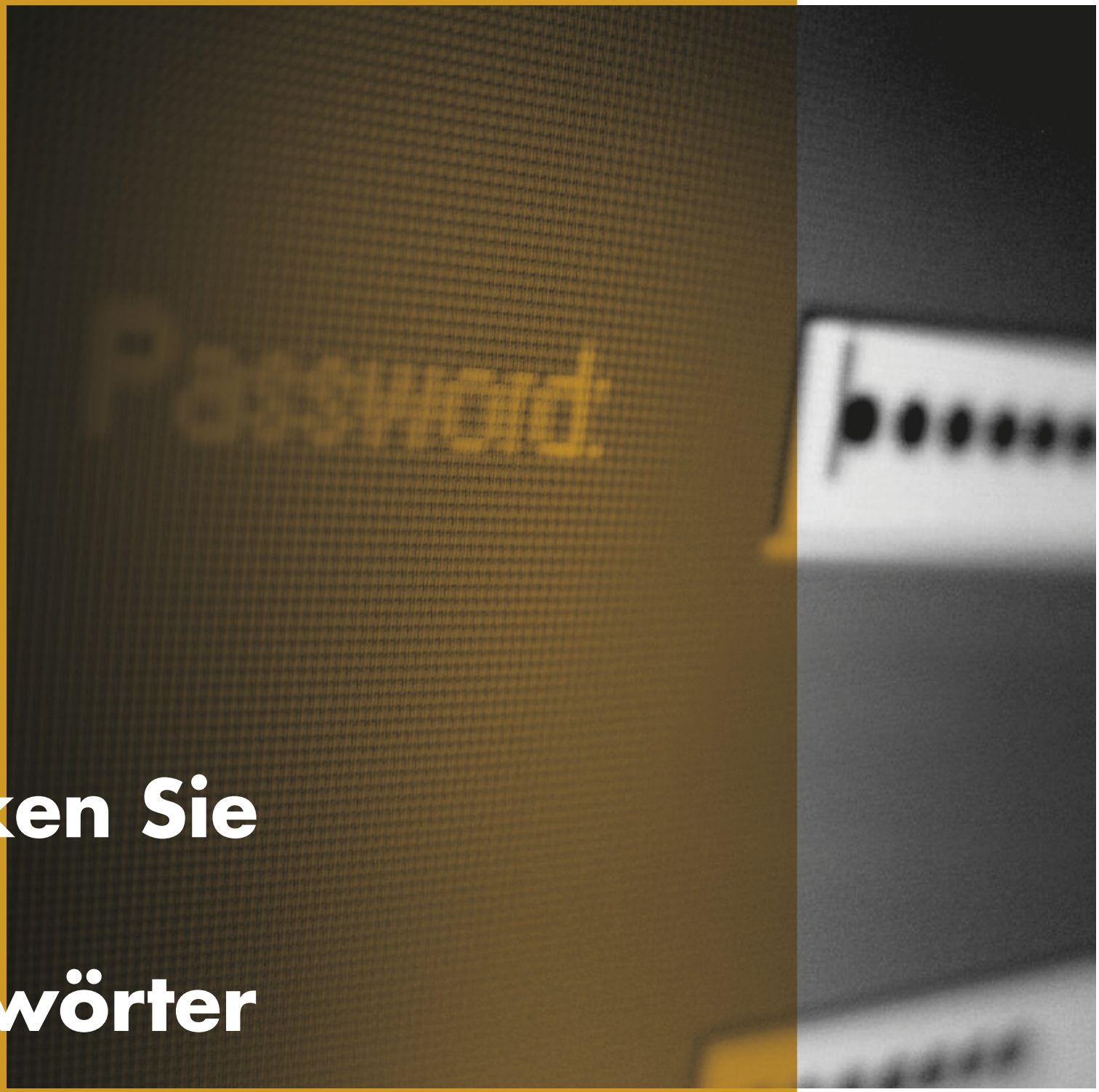
Viele moderne Geräte mit Windows 10 Pro und einer integrierten Webcam sind kompatibel mit Windows Hello. Das gilt auch für alle HP Notebooks und Convertibles. Durch das Scannen Ihres Gesichts bietet Ihnen Windows Hello eine Alternative zu einem Passwort, die Sie als eine Ihrer MFA-Anmeldedaten verwenden können.

1. Öffnen Sie: Einstellungen> Konten> Anmelde-Optionen
2. Wählen Sie unter „PIN“ die Option „Hinzufügen“, falls Sie noch keine Option eingerichtet haben.
3. Wählen Sie unter „Windows Hello“ die Option „Einrichten“ und befolgen Sie die Anweisungen auf dem Bildschirm, um Ihr Gesicht zu scannen.

9) HP Client Security Manager Gen4 erfordert Windows und Intel® oder AMD-Prozessoren der 8. Generation.
10) Das HP Manageability Integration Kit steht zum Download bereit auf http://www.hp.com/go/clientmanagement.

Abschnitt 2:

Stärken Sie Ihre Passwörter



Passwörter sind in unserem Alltag allgegenwärtig. Wir nutzen sie für nahezu alle unsere persönlichen und geschäftlichen Geräte, Services und Konten. Da sie die erste – und viel zu häufig auch die einzige – Verteidigungslinie zum Schutz unserer Identität und unserer Daten darstellen, kann die Verwendung schwacher Passwörter verheerende Folgen haben. Und trotzdem verwenden die wenigsten von uns starke und einzigartige Passwörter.

- 59 % der Befragten wissen, dass ein sicheres Passwort wichtig ist, und dennoch wählen 41 % ein Passwort, das leicht zu merken ist
- 91 % der Befragten sind sich der Risiken mehrfach verwendeter Passwörter bewusst, aber 55 % von ihnen ignorieren diese Risiken einfach
- Die Generation der Jahrtausendwende verwendet in der Regel stärkere Passwörter als die des Baby-Booms (65 % im Vergleich zu 45 %)[11]

Falls Ihr Gerät oder Service keine MFA unterstützt, besteht die nächstbeste Option darin, Ihr Passwort so stark wie möglich zu machen. Die meisten Menschen verwenden keine starken Passwörter, weil sie einfach nicht wissen, wie sie diese erstellen können, da sie davon ausgehen, es müsse eine zufällige Kombination aus Buchstaben, Zahlen und Symbolen sein. Aber es gibt bessere und einfachere Wege, um Ihren Passwortschutz drastisch zu steigern.

11) Quelle: LastPass, "New Research: Psychology of Passwords, Neglect is Helping Hackers Win", Katie Petrillo, May 1, 2018

Ziehen Sie Merksprüche numerischen Kombinationen vor.

Mnemonische Passphrasen sind sicherer als einfache Passwörter und einfacher zu merken als numerische Kombinationen. Wenn sie an Stelle einfacher Passwörter verwendet werden, ist es Hackern praktisch unmöglich, sie zu knacken.

1 Beginnen Sie mit einem einprägsamen Satz.

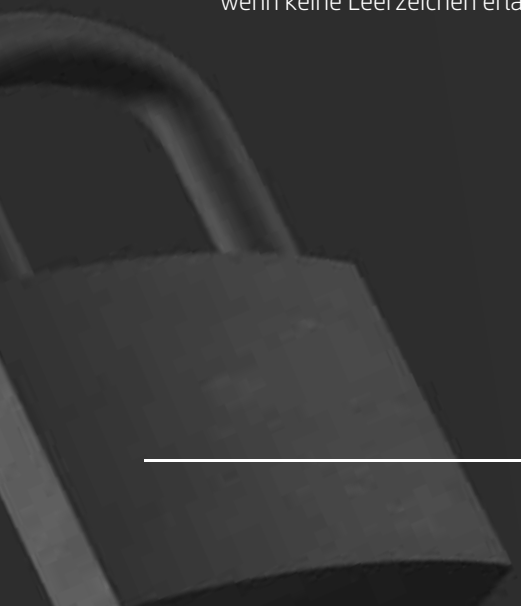
Nehmen Sie beispielsweise die ersten sechs Worte der berühmten Gettysburg-Rede von Abraham Lincoln: „Four score and 7 years ago“ ist eine einfache Passphrase. Das Zitat erfüllt die meisten Passwort-Standards: 8 bis 32 Zeichen, mit Groß- und Kleinbuchstaben und mindestens einer Zahl und einem Sonderzeichen (Leerzeichen oder Unterstriche, wenn keine Leerzeichen erlaubt sind).

2 Steigern Sie die Eigenartigkeit.

Erhöhen Sie die Anzahl der Zahlen und Sonderzeichen. Ändern Sie beispielsweise die Buchstaben in unserem vorherigen Beispiel folgendermaßen:
„4 $core @nd 7 Ye@rs ago“.

3 Personalisieren, nicht kopieren.

Indem Sie schlicht einen einfachen Zusatz an das Ende jeder Passphrase anhängen, können Sie Ihr Masterpasswort problemlos wiederverwenden, ohne Gefahr zu laufen, es doppelt zu nutzen. Für einen Facebook-Account können Sie beispielsweise „FB“ an das Ende der Passphrase anfügen, oder „IG“ im Falle von Instagram.



Verwenden Sie einen Passwort-Manager.

Laut Sicherheitsexperten zählten Passwort–Manager zu den besten Sicherheitspraktiken. Sie generieren und speichern lange, komplizierte Passwörter für jedes Ihrer Online-Konten – sodass Sie sich nichts merken müssen. In der Regel müssen Sie sich nur ein einziges Passwort, das Masterpasswort zu Ihrem „Tresor“, merken.
Die Einrichtung eines Passwort-Managers ist einfach und der Vorgang ist meistens immer derselbe:

1. Laden Sie die Software herunter und installieren Sie die Software und eine Erweiterung für Ihren Browser. Sie können auch eine App auf Ihr Mobilfunkgerät herunterladen.
2. Richten Sie mit einer E-Mail-Adresse und Ihrem Masterpasswort Ihr Konto ein.
3. Geben Sie die Details Ihrer verschiedenen Konten ein.

Für die meisten Passwort-Manager ist es erforderlich, dass Sie Ihre alten Passwörter manuell aktualisieren: Loggen Sie sich in Ihr jeweiliges Konto ein, gehen Sie zu Ihren Kontoeinstellungen und lassen Sie zu, dass Ihr Passwort-Manager ein neues, sichereres Passwort erstellt. Das Ersetzen Ihrer alten Passwörter kann zeitintensiv sein, aber die drastische Erhöhung Ihrer Sicherheit ist die Mühe wert.

Wählen Sie einen Passwort-Manager.

Es gibt zahlreiche kostenlose Passwort-Manager, wie Bitwarden, Dashlane und Enpass. Suchen Sie nach einem Passwort-Manager, der:

- Einfach in den Browser zu integrieren ist, den Sie am häufigsten verwenden.
- Es Ihnen erlaubt, die Passwort-Datei als verschlüsselte Datei zu speichern, sodass sie nicht ohne die vorherige Verifizierung der Benutzeridentität gelesen werden kann. Eine AES-256-Verschlüsselung oder stärker verwendet. Das ist ganz besonders wichtig.
- Eine Zwei-Faktor-Authentifizierung zum Zugriff auf den Passwort-Tresor unterstützt.
- Einen Notfallkontakt zuweist, der ebenfalls auf den Passwort-Tresor zugreifen kann.
- Gemeinsam mit dem Passwort zusätzliche Login-Daten speichert (d. h. Sicherheitsfragen, Telefonnummern, Konto-Details usw.)

Abschnitt 3:

Verwenden Sie Anti-Malware-Software

Ein PC ohne Virenschutz, der sich mit dem Internet verbindet, kann innerhalb von nur wenigen Minuten mit Malware infiziert werden.

Die unterschiedlichsten Arten von Malware könnten auf augenscheinlich seriösen Websites gehostet oder in E-Mail-Anhänge eingebettet sein. Und jeden Tag werden weitere, neue Arten von Malware entwickelt. Ihr PC wird kontinuierlich mit Viren bombardiert. Daher muss das Tool, das ihn schützt, leistungsfähig und gründlich sein und regelmäßig aktualisiert werden. Ein gutes Anti-Malware-Programm erfüllt alle drei Punkte.

Zusammengefasst lässt sich sagen, dass eine Anti-Malware-Software ein Programm ist, das dazu konzipiert wurde, Software-Viren (und andere bösartige Software wie Würmer, Trojaner, Adware und mehr) zu vermeiden, suchen, finden und entfernen. Ein typisches Anti-Malware-Programm scannt Ihr System regelmäßig und entfernt automatisch sämtliche Malware, die es entdeckt. Außerdem warnt es Sie vor gefährlichen Downloads und erinnert Sie an Software-Updates.

Wer also noch keine Anti-Malware-Software hat, sollte sich schnell eine besorgen.

Es gibt zahlreiche Anti-Malware-Produkte auf dem Markt. Falls Sie Windows 10 Pro verwenden, ist das Windows Defender Antivirus-Programm bereits installiert und aktiviert. Alternativ können Sie auch ein Anti-Malware-Programm eines Drittanbieters erwerben. Stellen Sie aber in jedem Fall sicher, dass Sie die Anweisungen des Herstellers zur Konfiguration automatischer Updates befolgen, sodass Sie stets über den aktuellsten Virenschutz verfügen.

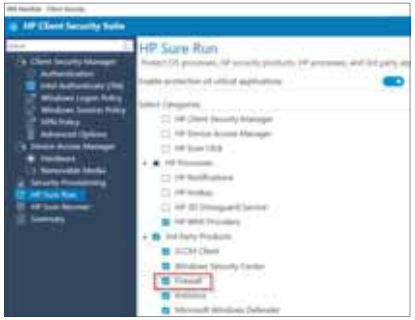
Immer aktiv.

Um effektiv zu sein, ist es ausschlaggebend, dass die Anti-Malware-Software kontinuierlich aktiv ist. Da Angreifer häufig zuerst Sicherheitsprogramme wie Anti-Malware angreifen, ist dieser Schritt nicht so einfach, wie er vielleicht scheint. In Windows 10 Pro können Sie überprüfen, ob Ihr Virenschutzprogramm aktiviert ist, indem Sie das Windows Defender Security Center öffnen.

1. Öffnen Sie vom Start-Menü aus das Windows Defender Security Center und gehen Sie zu „Home“.

2. Wenn das Virenschutzprogramm aktiviert ist, sehen Sie unter der Einstellung „Viren- und Bedrohungsschutz“ ein grünes Häkchen. Falls Sie ein Virenschutzprogramm eines Drittanbieters verwenden, klicken Sie auf „Virenschutz-Anbieter anzeigen“, um in der Windows-Systemsteuerung zusätzliche Informationen zum Status Ihres Virenschutzprogramms angezeigt zu bekommen.

Deaktivieren Sie Ihre Anti-Malware-Software niemals.



HP Elite-Produkte beinhalten HP Sure Run[1,2], eine zusätzliche Sicherheitsstufe, die gewährleistet, dass all Ihre kritischen Prozesse auf Ihrem PC, einschließlich Ihrer Virenschutzsoftware, in Betrieb sind. Jeder Prozess, der von Sure Run überwacht wird, wird automatisch neu gestartet, wenn er deaktiviert ist. So wird verhindert, dass Sie aufgrund einer deaktivierten oder abgestürzten Virenschutz-Software ungeschützt sind.

Sie müssen HP Sure Run lokal im HP Client Security Manager Gen4 aktivieren.

12) HP Sure Run ist für HP Elite-Produkte mit Intel-Prozessoren der 8. Generation oder mit AMD® verfügbar.

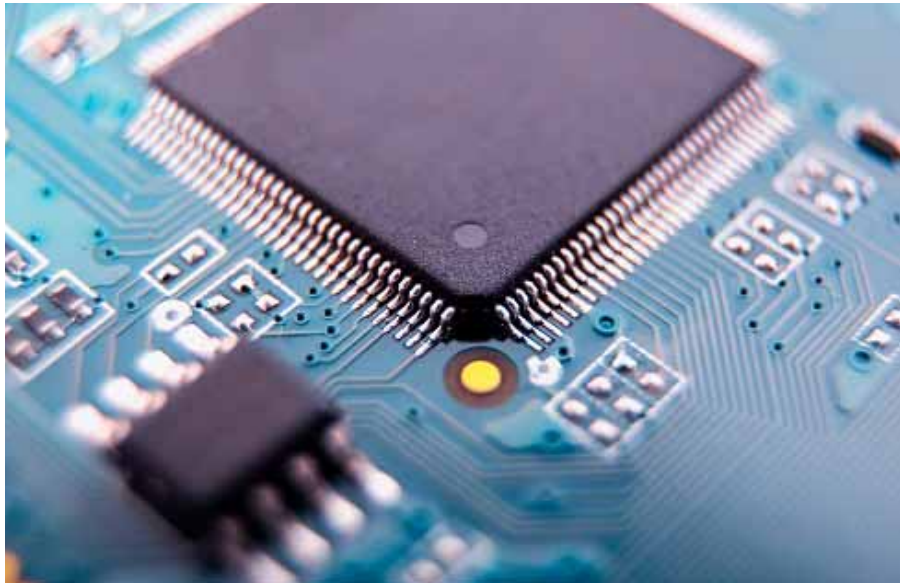
Abschnitt 4:

Halten Sie Ihre Software auf dem neuesten Stand

Anti-Malware ist nicht die einzige Software, die sich zunehmenden Bedrohungen gegenübersieht. Daher ist es von Bedeutung, dass Sie all Ihre Software-Programme auf dem neuesten Stand halten. Wenn Ihre Software nicht aktualisiert ist, kann es sein, dass sie nicht über wichtige Sicherheits-Patches verfügt, die für vor kurzem entdeckte Schwachstellen konzipiert wurden. Das gilt sowohl für das Betriebssystem (OS), wie Windows®, als auch für alle Anwendungen, die auf dem PC verwendet werden, wie Internet-Browser, Office-Anwendungen, Buchhaltungssoftware, Virenschutz-Software usw.

Bitte denken Sie auch daran, dass ältere oder eingestellte Software gegebenenfalls keine Sicherheits-Updates mehr erhält. Mit der Zeit finden Cyberkriminelle immer neue Schwachstellen in veröffentlichten Software-Programmen und machen sich diese zu Nutze. Sehen wir uns als Beispiel einmal das Betriebssystem an. Wenn wir nach einem Update für Windows 7 suchen, finden wir keine neue Software mehr. Der Grund hierfür ist, dass Windows 7 auch nicht mehr die aktuellste Windows-Version ist. Das Aufrüsten älterer Software ist nicht dasselbe, wie ein Update zur neuesten Version. Je älter Ihre Software ist, desto unsicherer ist sie.

> Je älter Ihre Software ist, desto unsicherer ist sie



Stellen Sie sicher, dass Sie Updates vornehmen.

Wenn Anbieter Lösungen für Schwachstellen finden, stellen sie diese Lösungen in Form von Software-Updates zu Verfügung. Die meisten Anwendungen verfügen über einen integrierten Update-Service, der gewährleistet, dass Sie informiert werden, wenn ein Update oder Patch verfügbar wird. Einige Software-Anbieter installieren die Updates sogar automatisch, sobald diese verfügbar werden. Windows 10 Pro, die aktuellste Version von Windows (und damit die sicherste), verfügt über einen automatischen Software-Update-Mechanismus, um das Betriebssystem und alle anderen Microsoft-Anwendungen auf dem neuesten Stand zu halten.

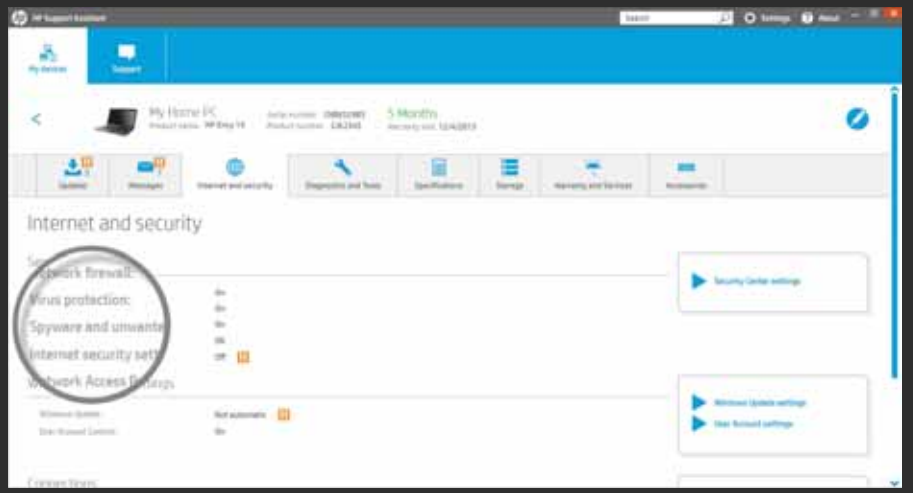
Um zu überprüfen, ob automatische Updates aktiviert sind:

1. Gehen Sie zu „Einstellungen“ und wählen Sie „Sicherheit aktualisieren“.
2. Wählen Sie unter „Windows Update“ die Option „Erweiterte Optionen“ und stellen Sie sicher, dass unter „Wählen, wie Updates installiert werden“, die Option „Automatisch“ aktiviert ist.
3. Stellen Sie sicher, dass unter „Wählen, wie Updates installiert werden“, die Option „Automatisch“ aktiviert ist.

Verwenden Sie einen Update-Manager.

Die Bandbreite an Software, die Ihr PC mit sich bringt, macht es schwer, sicherzustellen, dass *alles* auf dem neuesten Stand ist. Aus diesem Grund stellen viele PC-Anbieter vorinstallierte Tools zu Verfügung, die automatisch alle Software- und Firmware-Updates für das System erfassen. In Systemen von HP heißt das Tool HP-Support Assistant.

Für Anwendungen von Drittanbietern wird die Update-Funktion oftmals von einer kleinen Update-Anwendung ausgeführt, die beim Systemstart aktiviert wird. Durch diese Helfer-Tools dauert der Systemstart etwas länger, dafür müssen Sie nicht auf den Websites der Anbieter nach den jeweiligen Updates suchen. Falls Sie eine Software verwenden, die nicht automatisch nach Updates sucht, oder wenn Sie sich nicht sicher sind, überprüfen Sie auf der Website des Herstellers die Versionsnummern und aktualisieren Sie Ihre Software, falls erforderlich.



Abschnitt 5:

Sichern Sie Ihren Browser

Browser wie Internet Explorer oder Chrome™ sind der Hauptweg ins Internet und somit das beliebteste Ziel für Hacker. In der Regel erfolgen die Angriffe durch einen ungewollten oder absichtlichen Klick auf einen Link, der ein Schadprogramm in Gang setzt, das als Malware bezeichnet wird.

Mit einigen wenigen Schritten können Sie die Wahrscheinlichkeit eines Malware-Angriffs über den Browser deutlich reduzieren.

Verwenden Sie einen gesicherten Browser.

Internet Explorer, Edge und Chrome bieten alle effiziente Sicherheitsfunktionen für Windows. So verwenden Edge und Internet Explorer 11 beispielsweise Microsoft SmartScreen, um auf jeder Seite eine Reputationsprüfung durchzuführen und alle Seiten zu blockieren, die den Verdacht erwecken, eine Phishing-Site zu sein. Zusätzlich profitiert Internet Explorer auf kommerziellen HP-PCs von der zusätzlichen Sicherheit von HP Sure Click: Wann immer eine neue Registerkarte geöffnet wird, führt HP Sure Click diese auf einer isolierten virtuellen Maschine aus. Das bedeutet, dass sämtliche bösartige Software in der Registerkarte gefangen ist und zerstört wird, wenn Sie Ihren Browser[13] schließen.

Halten Sie ihn auf dem neuesten Stand.

Aktivieren Sie in den Einstellungen automatische Browser-Updates. Wie bereits erwähnt, gewährleisten Sie damit, dass auf Ihrem Browser alle aktuellen Sicherheitsupdates angewandt werden. So wird Ihr Router deutlich sicherer und es wird wahrscheinlicher, dass Malware-Angriffe fehlschlagen.

In Edge werden immer dann Updates angewandt, wenn Windows aktualisiert wird. Wenn Sie dennoch überprüfen möchten, ob Sie ein Update für Edge benötigen, gehen Sie zu:

- Start
- Einstellungen
- Updates und Sicherheit
- Windows Update
- Nach Updates suchen

13) HP Sure Click ist auf den meisten HP-PCs verfügbar und unterstützt Microsoft® Internet Explorer und Chromium™. Zu den unterstützten Anhängen gehören Microsoft Office (Word, Excel, PowerPoint) und PDF-Dateien im Schreibschutz-Modus, wenn Microsoft Office oder Adobe Acrobat installiert sind.

Beachten Sie Warnhinweise.

Die meisten der gängigen, modernen Browser verfügen über eine grundlegende Erkennungsschwelle für betrügerische Websites und zeigen einen Warnhinweis an, wenn der Verdacht einer Bedrohung besteht. Einige Browser bieten auch Funktionen für eine URL-Autokorrektur, um zu verhindern, dass Sie zu einer häufig falsch geschriebenen Domain navigieren (wo oftmals bösartige Software und betrügerische Sites gehostet werden).

In Edge gehen Sie zu „Erweiterte Einstellungen“ > „Datenschutz“ und aktivieren Sie die Einstellungen „Einen Web-Service zur Lösung von Navigationsfehlern verwenden“

Beschränken Sie Inhalte und Plug-Ins.

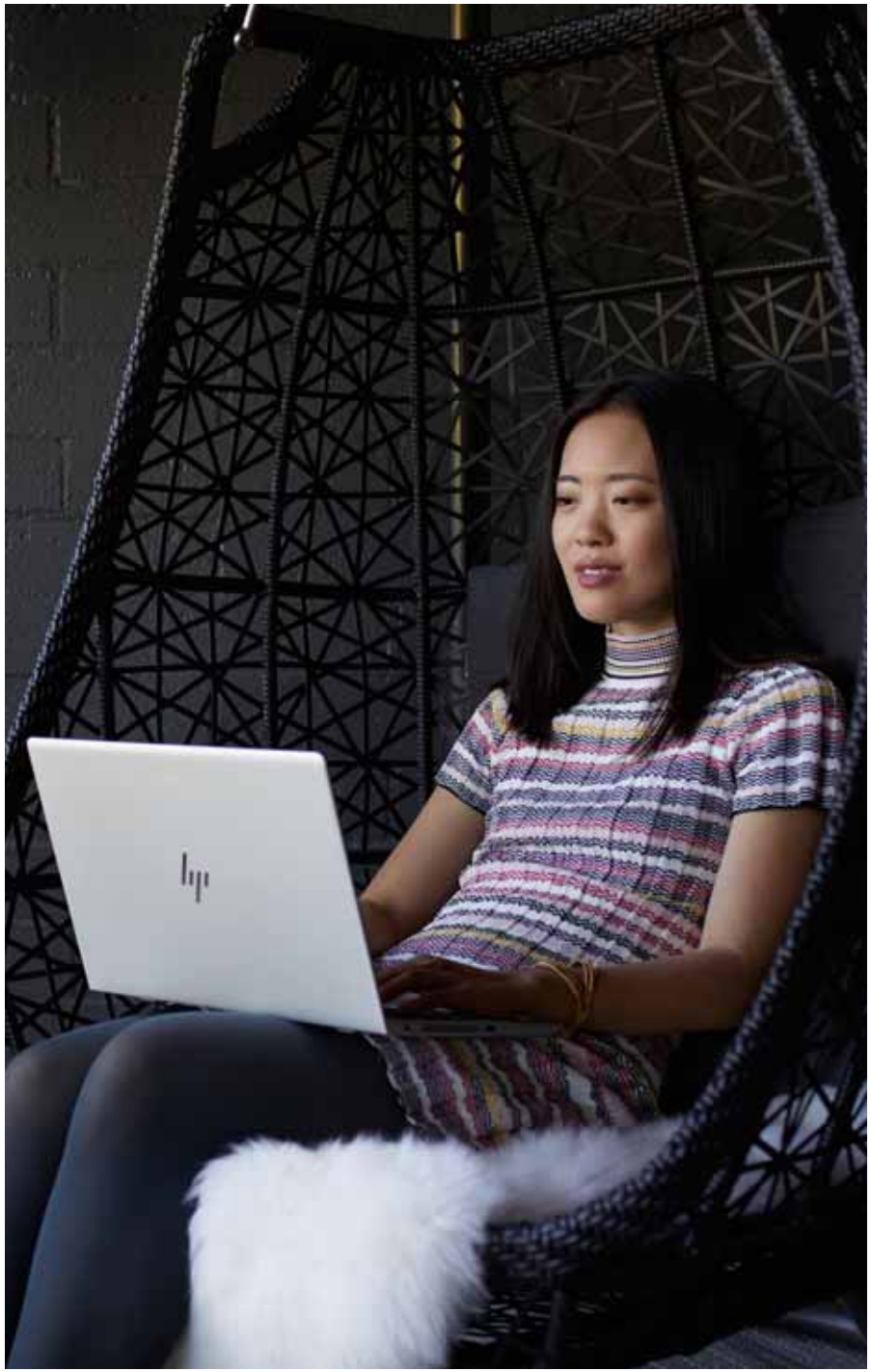
Viele der Browser-Add-ons (wie Flash und JavaScript) sind für inhaltsreiche Websites und Web-Programme unerlässlich. Leider stellt ihr umfassenderer Zugriff auf Ihr System eine Schwachstelle dar.

Durch ihre standardmäßige Deaktivierung ist es erforderlich, dass Sie Ihre Zustimmung geben müssen, bevor eine Website Add-ons nutzen kann. Dies gewährleistet, dass nur Websites, denen Sie vertrauen, die Funktionen der Add-ons nutzen können.

Gehen Sie in IE zu: Werkzeuge (Zahnrad-Symbol) > Internet Optionen > Sicherheit > Internet > Stufe anpassen > Scripting. Sie können JavaScript deaktivieren, indem Sie einfach die Option „Deaktivieren“ wählen. Oder Sie richten Ihre Einstellungen so ein, dass IE eine Anfrage stellt, wenn eine Website versucht, Add-ons zu verwenden. Wählen Sie hierzu die Option „Abfrage“.

Abschnitt 6:

Router-Sicherheit und privates Netzwerk



Der Router ist die erste Sicherheitslinie bei Eingriffen in ein Netzwerk. Jeder, der sich mit dem Internet verbindet, nutzt hierfür einen Router. Dieses Hardwaregerät, entweder kabelgebunden oder drahtlos (Wi-Fi®), ermöglicht die Kommunikation zwischen Ihrem lokalen Netzwerk (d. h. Ihrem PC und möglicherweise anderen verbundenen Geräten) und dem Internet. Daher können Sie Ihre PCs, Drucker und Daten am besten vor böswilligen Angriffen schützen, indem Sie das höchstmögliche Sicherheitsniveau Ihres Routers aktivieren.

> Router wurden als das Gerät genannt, das am häufigsten IoT-Angriffen zum Opfer fällt.[14]

Da SÄMTLICHE Daten, die in oder aus Ihrem Haus oder Unternehmen übertragen werden, durch Ihren Router fließen, einschließlich Ihrer E-Mail- und Kreditkarten-Daten, sind Router schon lange ein beliebtes Angriffsziel für Hacker. Im 2018 Internet Security Threat Report von Symantec werden Router als das Gerät genannt, das am häufigsten IoT-Angriffen zum Opfer fällt. Hacker können Malware oder Designfehler nutzen, um ihre Identität zu verschleiern, Bandbreite zu stehlen, Ihre Geräte in Botnet-Zombies zu verwandeln oder noch Schlimmeres zu tun. Sie können sich auch jedes ungesicherte Gerät zu Nutze machen.

14) Quelle: Symantec Corporation, 2018 Internet Security Threat Report, 2018

Sichern Sie Ihr Netzwerk.

Leider bieten viele Anbieter weiterhin sowohl gesicherte als auch ungesicherte Router-Konfigurationen an. Wenn ein Router ungesichert ist (d. h., wenn er ohne ein Administrator-Passwort Verbindungen zulässt), kann sich jeder mit dem Router verbinden und auf Ihr lokales Netzwerk zugreifen. Ein Hacker könnte Ihre Passwörter ändern, Sie ausspionieren oder sogar auf Dateien zugreifen, die auf einer mit dem Netzwerk verbundenen Festplatte gespeichert sind.

Sichern Sie Ihren Router stets mit personalisierten Administrator-Passwörtern, indem Sie die Tipps in Abschnitt 2 befolgen: Stärken Sie Ihre Passwörter. Im folgenden Screenshot wird gezeigt, wie Sie für die meisten Router Passwörter einrichten können, um diese im Netzwerk zu sichern.

Konfigurieren Sie die Verschlüsselung.

Bei Wireless-Routern sind Passwörter nur die halbe Miete – die Wahl der richtigen Verschlüsselungsebene ist ebenso wichtig. Die meisten Wireless-Router unterstützen vier Standards für die drahtlose Verschlüsselung: WEP (am schwächsten), WPA (stark), WPA2 (stärker), und WPA3 (am stärksten). Wählen Sie den höchsten Verschlüsselungsstandard, den Ihr Router unterstützt.

Im folgenden Screenshot wird gezeigt, wie Sie auf Ihrem Router die entsprechende Verschlüsselungsebene einstellen können. Um dies zu tun, müssen Sie sich als Administrator des Routers anmelden und zu den Verschlüsselungseinstellungen navigieren (der Pfad ist je nach Router-Anbieter unterschiedlich).

Halten Sie die Firmware auf dem neuesten Stand.

Viele Router-Hersteller stellen regelmäßig Software-Updates zur Verfügung, um Sicherheitsprobleme zu beheben. Daher gilt auch hier, was wir in Zusammenhang mit der PC-Software besprochen haben: Die Wahrscheinlichkeit, dass ein Router von Malware infiziert wird, ist wesentlich geringer, wenn er auf dem neuesten Stand ist. Die meisten Router-Anbieter führen Firmware-Updates automatisch durch, ohne dass der Kunde diese Aktion ausführen muss. Neuere Router-Modelle bieten eventuell auch eine mobile App, die Sie wie jede andere App auf Ihr Mobilfunkgerät laden können, um nach Updates zu suchen. Wenn Ihr Router-Anbieter jedoch keine automatischen Firmware-Updates anbietet, sollten Sie die Website des Herstellers besuchen, zu „Support“ gehen und das richtige Update ermitteln, indem Sie den spezifischen Modellnamen und die ID Ihres Routers eingeben (diese finden Sie in der Regel auf dem Router selbst).

Verwenden Sie virtuelle private Netzwerke (Virtual Private Networks, VPNs).

Ein virtuelles privates Netzwerk (VPN) ist ein Server, mit dem Sie sich verbinden, um Ihre externen Internet-Aktivitäten umzulenken. Ein VPN bietet mehr als die reine Sicherung Ihrer Hardware innerhalb Ihres Unternehmens. VPNs können Ihre Identität und Ihre Daten schützen. Ziel eines VPN ist es, eine massenkompatible Möglichkeit zur privaten Nutzung des Internets zu bieten (was allerdings nicht immer mit anonym gleichzusetzen ist). Sämtlicher Datenverkehr, der Ihre VPN-Verbindung durchläuft, ist sicher und kann – theoretisch – von niemandem abgefangen werden. Mehr Informationen zu VPNs und ihren Vorzügen finden Sie in Abschnitt 7.

Abschnitt 7:

Schützen Sie sich im öffentlichen Wi-Fi®

Heutzutage ist öffentliches Wi-Fi® allgegenwärtig. Flughäfen, Bars, Shopping-Malls und Event-Outdoor-Parks, überall dort gibt es per Hotspot freies Internet für alle. Hotspots sind unglaublich praktisch – und unglaublich gefährlich.

Benutzer, die sich mit diesen Hotspots verbinden, teilen sich ein Netzwerk. Das bedeutet, es besteht eine reelle Chance, dass sich jemand den ungesicherten Datenverkehr zu Nutze machen könnte. Ein Hacker kann sogar einen eigenen Hotspot einrichten und versuchen, Benutzer in sein betrügerisches (ähnlich benanntes) Netzwerk zu locken. So können unverschlüsselte Datenströme ausspioniert oder Man-in-the-Middle-Attacken ausgeführt werden, bei denen die Verschlüsselung umgangen wird.

Sie sollten immer davon ausgehen, dass Ihre Kommunikationen ungesichert und öffentlich sind, wenn Sie ein offenes Netzwerk verwenden. Wenn Sie das Netzwerk aber nutzen müssen, weil keine anderen Alternativen bestehen, gibt es Möglichkeiten, Ihre Gefährdung zu minimieren.

Beschränken Sie Ihre Aktivität.

Übertragen Sie keine hochvertraulichen Materialien wie Unternehmensunterlagen, E-Mails oder Passwörter und verwenden Sie keinerlei Banking- oder Buchhaltungsanwendungen oder -Portale.

Sehen Sie sich nach einem Plan B um.

Nutzen Sie, falls möglich, halboffene Verbindungen, die zumindest passwortgeschützt sind. Dabei handelt es sich in der Regel um verwaltete Netzwerke, was bedeutet, dass der Anbieter ein Interesse daran hat, das Netzwerk sicher zu halten (z. B. Airline-Lounges)

Nutzen Sie nur verschlüsselte Seiten.

Stellen Sie sicher, dass Sie mit einem Web-Server verbunden sind, der anhand des HTTPS-Protokolls (https://) einen verschlüsselten Datenverkehr unterstützt, anstatt das ungesicherte Plain Text HTTP-Protokoll zu verwenden. Überprüfen Sie die URL der Website: Ein moderner Browser verfügt in der Regel über ein Symbol in der URL-Leiste, das anzeigt, wenn HTTPS vorhanden und das Zertifikat gültig ist (oftmals ein Schloss-Symbol oder die Farbe Grün). Durch Klicken auf diesen Bereich erscheint ein Dialogfenster, das weitere Informationen zur Verschlüsselungsebene enthält.

Leiten Sie sämtlichen Datenverkehr durch ein VPN.

Wie wir im vorherigen Abschnitt bereits erwähnt haben, kann ein VPN dabei helfen, Ihre Daten zu schützen, wenn Sie Ihrer Netzwerkverbindung nicht trauen können, beispielsweise, wenn Sie ein öffentliches Wi-Fi®-Netzwerk verwenden. Ein VPN-Tunnel verschlüsselt Ihre Daten durchgängig und stellt so sicher, dass ein potenzieller Abfänger der Daten nicht in der Lage ist, Ihre Aktivität zu interpretieren. Nicht alle VPNs sind gleich konzipiert, daher müssen Sie das VPN wählen, das sich am besten für Ihre Preisklasse und Ihr Gerät eignet. Kostenlose VPNs verfügen oftmals nur über eine beschränkte verfügbare Bandbreite und einfache Verschlüsselungsprotokolle, was bedeutet, dass sich Ihre Browser-Geschwindigkeit verringert und Sie gegebenenfalls nicht vor allen Bedrohungen geschützt sind. Trotzdem ist ein seriöses kostenloses VPN in jedem Falle immer noch besser als gar kein VPN.

Abschnitt 8:

Stoppen Sie visuelle Hacker

Visuelle Hacking-Angriffe ereignen sich, wenn vertrauliche Informationen an öffentlichen Orten auf einem Bildschirm angezeigt werden und Konkurrenten, Identitätsdiebe oder andere skrupellose Personen diese sehen, erfassen und zu ihren Gunsten verwenden. Sogar zufällige Schaulustige stellen eine potenzielle Bedrohung dar. Alles – von Passwörtern und Kontonummern bis hin zu Finanzdaten und vertraulichen Unternehmensdaten – ist gefährdet, und keine Sicherheitssoftware ist ausreichend, um diese Daten-Voyeure davon abzuhalten, einen Blick zu riskieren.

Während der moderne Arbeitsplatz zunehmend von traditionellen Büros an entlegene und öffentliche Orte verlegt wird, ist die Gefahr, virtuell gehackt zu werden, größer als jemals zu vor. Tatsächlich ist virtuelles Hacking sogar eine der am meisten unterschätzten und technisch einfachsten Bedrohungen, denen sich Unternehmen heutzutage gegenübersehen. Es ist einfach, effektiv und bleibt meistens unentdeckt, bis es bereits zu spät ist.

Eine Umfrage des Ponemon Institute[1] ergab:

- 91 % aller visuellen Hacking-Angriffe waren erfolgreich
- 68 % aller visuellen Hacking-Angriffe wurden vom Opfer nicht bemerkt
- 52 % der vertraulichen Daten wurden direkt von Gerätebildschirmen abgelesen

Achten Sie auf Ihr Umfeld.

Gehen Sie beim Arbeiten an öffentlichen Orten stets davon aus, dass Ihnen jemand über die Schulter sehen könnte, und wählen Sie Ihre Arbeiten entsprechend aus.

Beschränken Sie Ihr Ausgesetztsein.

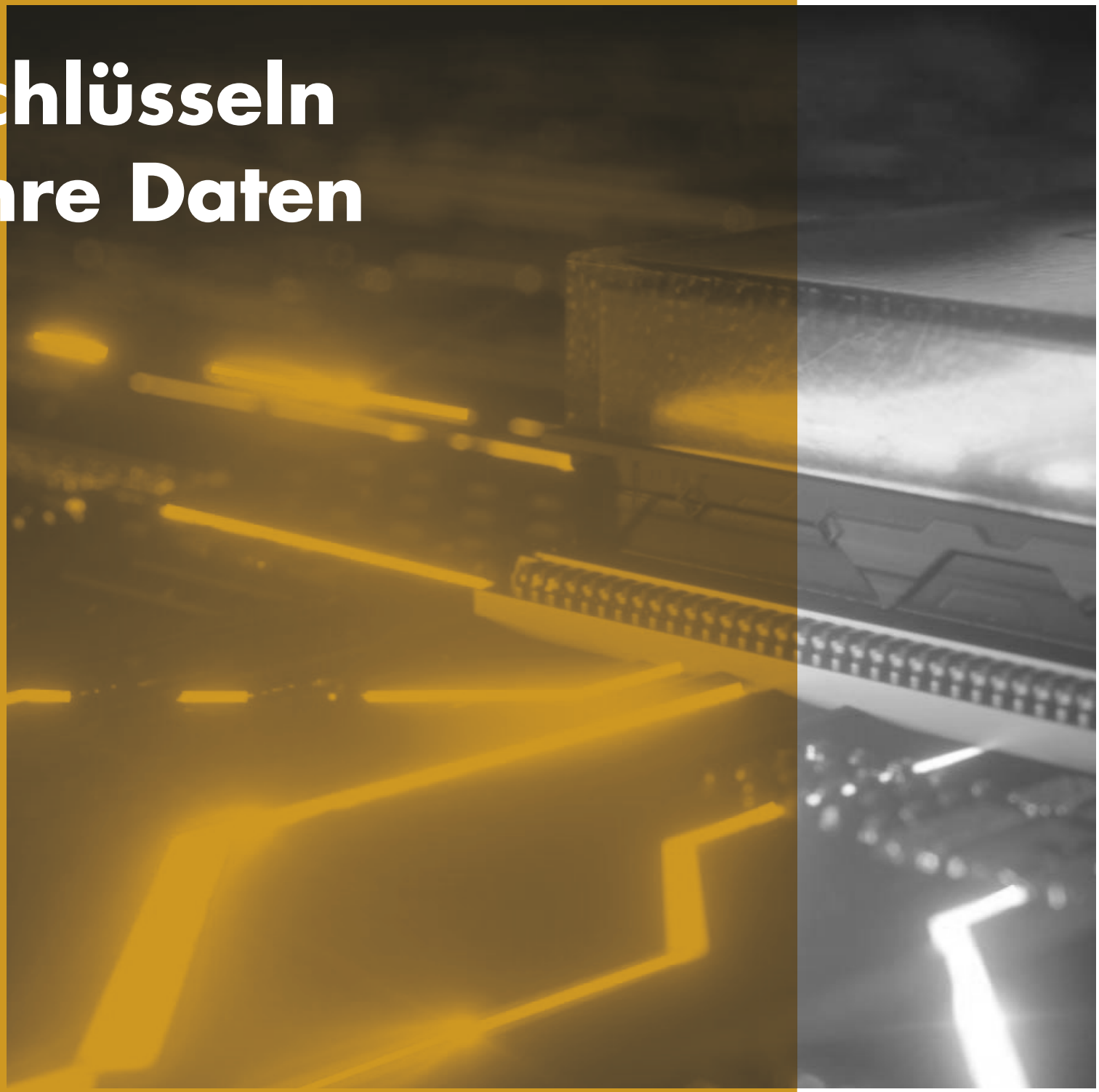
Verwenden Sie einen Sichtschutz, der den Betrachtungswinkel Ihres Bildschirms reduziert, sodass ein potenzieller visueller Hacker die Bildschirmanzeige nicht sehen kann, ohne direkt davor zu stehen. Ein externer Blickschutzfilter ist eine einfache Möglichkeit, diese Sicherheitsmaßnahme zu ergreifen. Er wird über Ihrem Bildschirm angebracht und kann entfernt werden, wenn Ihre Bildschirmanzeige von mehreren Personen gesehen werden soll.

Alternativ können Sie auch einen integrierten Datenschutzbildschirm verwenden, der den Prozess vereinfacht, da er nicht wie der externe Blickschutzfilter immer wieder angebracht und aufbewahrt werden muss. Viele PCs von HP verfügen über HP Sure View Gen2[15], einen integrierten Datenschutzbildschirm, der als Option konzipiert wurde, um visuelles Hacking zu unterbinden. Er funktioniert durch eine dynamische Modifizierung der LCD-Pixel-Struktur auf molekularer Ebene. Dadurch kann er mit nur einem Tastenklick aktiviert bzw. deaktiviert werden und die Leistung in sowohl hellen als auch dunklen Umgebungen verbessern.

15) Der integrierte Datenschutzbildschirm von HP Sure View ist eine optionale Funktion, die beim Kauf konfiguriert werden muss und die für eine Ausführung im Querformat konzipiert ist.

Abschnitt 9:

Verschlüsseln Sie Ihre Daten



Wenn ein PC verloren geht oder gestohlen wird, ist die Festplatte der erste Angriffspunkt. Nur ein paar Schräubchen halten sie an ihrem Platz, sodass sie einfach ausgebaut und in einen anderen PC eingebaut werden kann. Falls Sie Ihre Daten nicht ausreichend geschützt haben, ist das Lesen Ihrer Festplatte so einfach wie das Lesen eines Buches.

Verschlüsselung gewährleistet, dass die gewonnenen Daten vollständig unlesbar bleiben. Verschlüsselung ist der Prozess der Datenkodierung, um diese für jeden unlesbar zu machen, der nicht über den geheimen Entschlüsselungscode verfügt. Das bedeutet, dass ein Computer mit einer verschlüsselten Festplatte zwar gestohlen, aber nicht genutzt werden kann. Ein gestohlener Computer ist zwar ärgerlich, aber doch immer noch wesentlich besser, als wenn Ihre geschäftlichen oder privaten Daten für immer in die falschen Hände gelangen würden.

Aktivieren Sie die Software-Verschlüsselung.

Windows 10 Pro unterstützt die Passwort-Verschlüsselung Ihrer Festplatte, indem Ihre Login-Daten als Schlüssel verwendet werden. Dadurch wird sichergestellt, dass ein Hacker Ihren Benutzernamen und Ihr Passwort benötigt, um auf Ihre Daten zugreifen zu können.

Stellen Sie sicher, dass Sie ein starkes Passwort für Ihr Benutzerkonto haben:

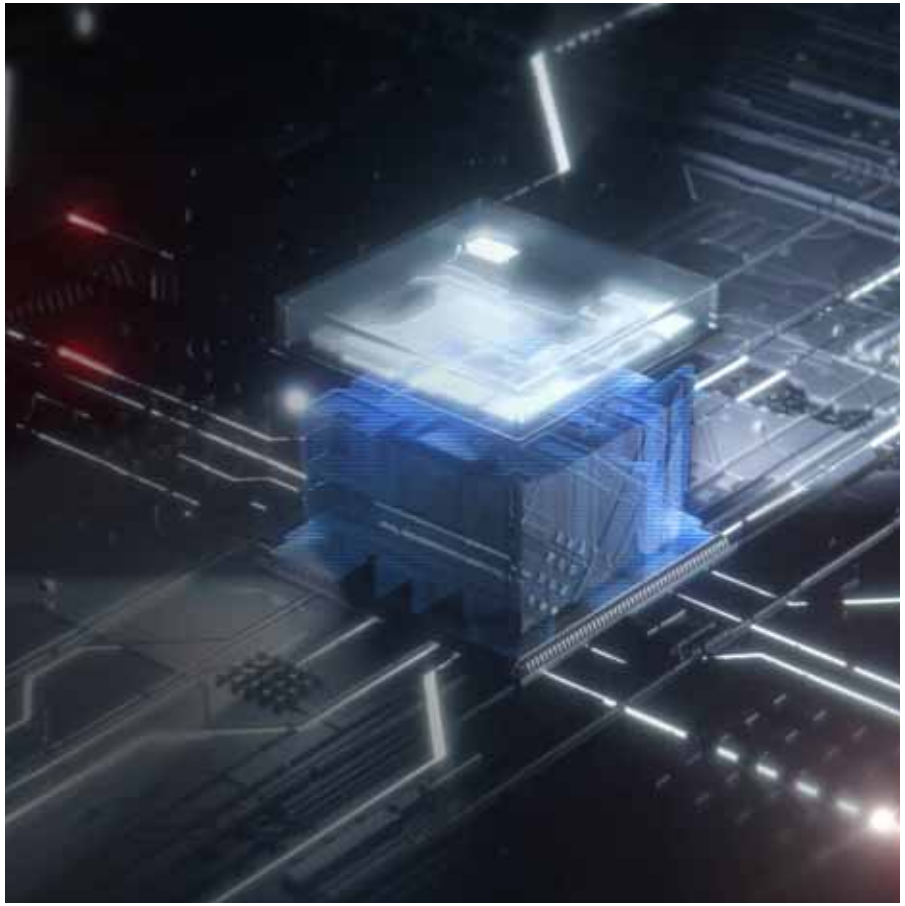
1.
   - Einstellungen > Konten> Anmelde-Optionen > Passwort

2. Aktivieren Sie, falls verfügbar, den Trusted Platform Manager (TPM), der wiederum einen Sicherheitschip in Ihrem PC aktiviert, um Ihre neuen Passwörter und Daten auf der Festplatte zu verschlüsseln:
   - Einstellungen > Update und Sicherheit > Windows Sicherheit > Gerätesicherheit > Prozessor

3. Aktivieren Sie die Verschlüsselung und stellen Sie so sicher, dass Ihre Daten nicht ohne Ihre Anmeldedaten eingesehen oder kopiert werden können:
   - Einrichtungen > Update und Sicherheit > Laufwerkverschlüsselung

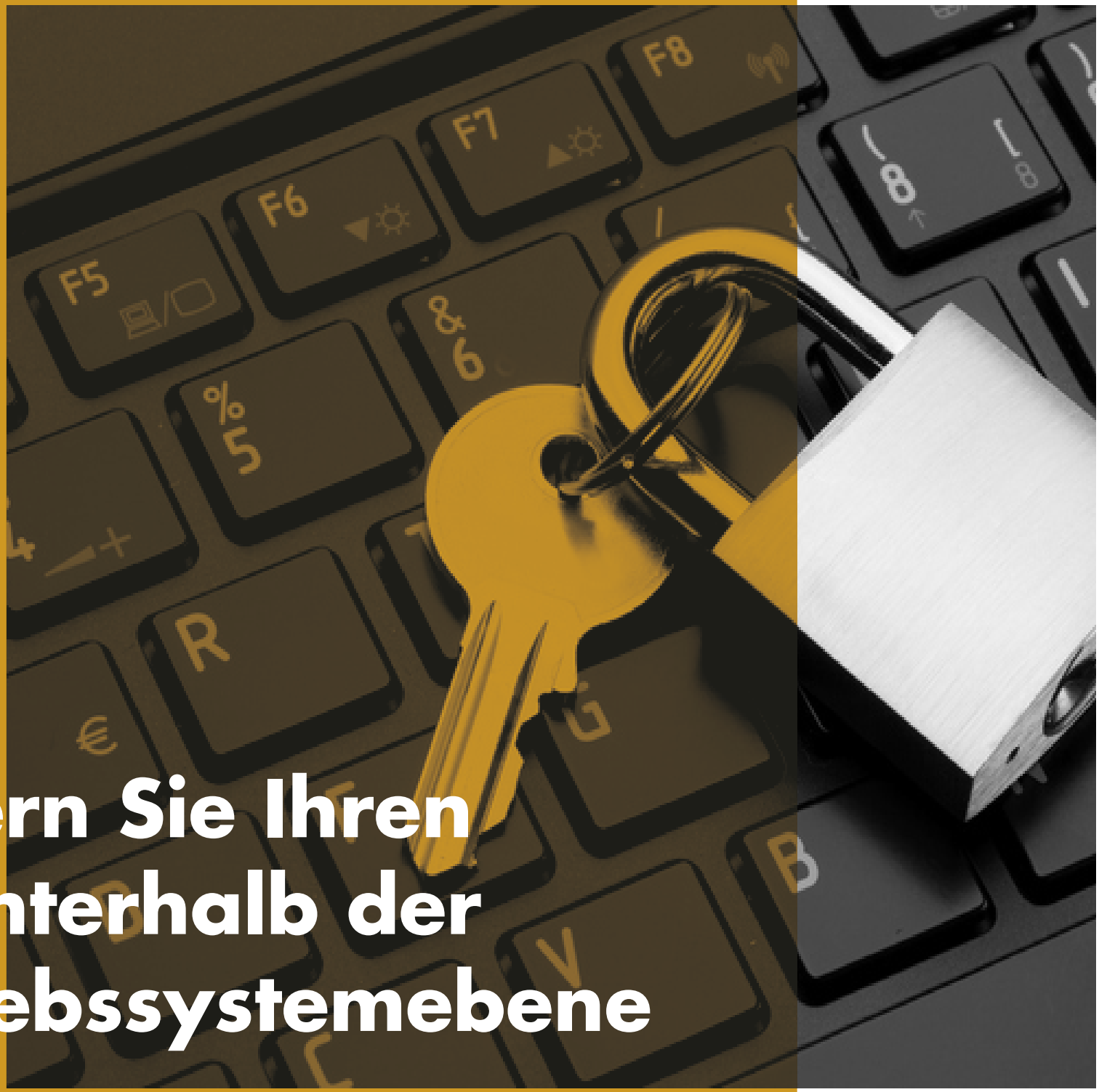
Nutzen Sie die Vorteile der Hardware-Verschlüsselung.

BitLocker ist eine Funktion von Windows 10 Pro und bietet eine Software-Verschlüsselung, die mit einem Hardware-Schlüssel entschlüsselt wird. Geräte, die über einen TPM-Chip verfügen, wie HP Notebooks, können ohne zusätzliche Hardware verschlüsseln. Der TPM verhindert den Zugriff auf verschlüsselte Daten, falls er bemerkt, dass das System manipuliert wurde, während es ausgeschaltet war. Geräte ohne TPM können BitLocker ebenfalls nutzen, aber in diesem Fall ist ein Wechseldatenträger, wie beispielsweise ein USB-Stick, erforderlich, der als Schlüssel dient.



Abschnitt 10:

Sichern Sie Ihren PC unterhalb der Betriebssystemebene



Das BIOS (Basic Input Output Software) ist eine Software, die den Computer startet und beim Laden des Betriebssystems hilft. Indem sie diese Basissoftware infizieren, können Spione Malware platzieren, die immer aktiv und von Virenschutzprogrammen unentdeckt bleibt. Diese Art von Malware wird nicht einmal entfernt, wenn die Festplatte gelöscht oder ein neues Betriebssystem installiert wird.

Wenn es einem Hacker gelingt, auf Ihr BIOS zuzugreifen, gehört ihm praktisch jeder Aspekt Ihres PCs.

Der Hacker kann nun Ihre Daten filtern oder das System funktionsunfähig machen, indem er die Firmware modifiziert. Um dies zu beheben, müsste die komplette Systemplatine ersetzt werden.
Für HP Elite und Pro PCs kann HP Sure Start automatisch das BIOS von Malware, Rootkits oder sonstiger Korrumpierung schützen, indem eine zusätzliche Sicherheitsstufe eingeführt und eine vertrauenswürdige Basis für die Sicherheit Ihres PCs geschaffen wird.[16]

Verpassen Sie kein Update.

Wie bereits in Abschnitt 4 erwähnt, stellen Software-Updates sicher, dass neu entdeckte Schwachstellen behoben werden. Das BIOS bildet hierbei keine Ausnahme. Da die meisten BIOS-Implementierungen innerhalb einer Belegschaft oder Benutzerbasis denselben Quellcode verwenden, ist es wahrscheinlich, dass eine entdeckte Schwachstelle in zahlreichen Implementierungen innerhalb der PC-Anbieter-Landschaft auftritt. OEM-Tools wie HP-Support Assistant suchen automatisch nach Updates. Ansonsten können Sie auch auf der Website des Herstellers nach BIOS-Updates suchen.

Erforschen Sie das BIOS.

Die BIOS-Standardeinstellungen sind ein Kompromiss zwischen Sicherheit und Benutzerfreundlichkeit. Um Ihr System gegen viele verschiedene Methoden zur Übertragung von bösartiger Software zu schützen, ist es sinnvoll, auf einige Aspekte der Funktionalität zu verzichten.

Der Zugriff auf das BIOS kann je nach Hersteller unterschiedlich erfolgen, aber in der Regel wird während des anfänglichen Hochladens eine Funktionstaste gedrückt (bei HP Notebooks F10 oder FN-10).

16) HP Sure Start Gen4 ist für HP Elite und HP Pro 600 Produkte mit Intel®- oder AMD-Prozessoren der 8. Generation verfügbar.

Richten Sie ein BIOS-Passwort ein.

Um zu verhindern, dass Ihre BIOS-Einstellungen von unbefugten Benutzern modifiziert werden, wird empfohlen, ein BIOS-Passwort einzurichten:

- Zum Beispiel: Sicherheit > Administrator-Tools > BIOS Administrator-Passwort erstellen

Es ist sehr wichtig, dass Sie sich das BIOS-Passwort merken, da es nicht umgangen oder wiederhergestellt werden kann.

Richten Sie ein Passwort für den Systemstart ein.

Um die Sicherheit noch weiter zu erhöhen, kann ein Passwort für den Systemstart erstellt werden. Dieses muss dann bei jedem Einschalten des PCs eingegeben werden, bevor das System irgendetwas ausführt. Ebenso wie das BIOS-Passwort kann auch das Passwort für den Systemstart nicht einfach wiederhergestellt werden, und wenn Sie es vergessen, wird das Gerät unbrauchbar.

Beschränken Sie ungenutzte Funktionen.

In BIOS gibt es einige Einstellungen, die für eine maximale Sicherheit berücksichtigt werden sollten. Sie verringern gegebenenfalls die Funktionalität oder reduzieren die Zugänglichkeit. Dafür sorgen sie aber unterhalb der Betriebssystemebene für ein Sicherheitsniveau, das mit Software nicht erreicht werden kann:

1. Entfernen Sie externe und optische Geräte aus der Startreihenfolge (z. B.: Erweitert > Startoptionen). Deaktivieren Sie insbesondere den Start von USB-Datenträgern, Netzwerken (PXE) und optischen Laufwerken, da durch diese Malware aus externen Quellen hochgeladen werden kann. Falls das Starten dieser Geräte erforderlich ist, können Sie die jeweilige Funktion bei Bedarf aktivieren.
2. Deaktivieren Sie die Legacy-Unterstützung (z. B.: Erweitert > Secure Boot-Konfiguration) und aktivieren Sie Secure Boot.
3. Aktivieren Sie die Funktion „GPT der Systemfestplatte speichern/wiederherstellen“ (z. B.: Sicherheit > Festplatten-Dienstprogramme).
4. Aktivieren Sie DriveLock und richten Sie ein Passwort ein.

Fazit

Nie zuvor waren kleine und mittelständische Unternehmen derart vielen digitalen Bedrohungen ausgesetzt wie heute. Die gute Nachricht ist, dass ein Großteil der Hard- und Software, die Sie besitzen, über unzureichend genutzte Sicherheitsfunktionen verfügt, mit denen Sie sich gegen diese Bedrohungen wehren können. Außerdem gibt es eine beispiellose Anzahl an Produkten und Services, die hochmoderne Sicherheitsinnovationen bieten, um Sie gegen die Gefahren von morgen zu schützen. Von hardwarebasierten Sicherheitsvorkehrungen auf zeitgenössischen Geräten bis hin zu Software mit automatischen Updates – wer sich heute für eine kluge Investition in verbundene, sichere Geräte entscheidet, wird in Zukunft sicherlich davon profitieren. HP konzipiert Sicherheitslösungen, die sich die Stärken von Windows 10 Pro zu Nutze machen, indem sie die integrierten Sicherheitsfunktionen mit separaten Hardware-Erweiterungen und einem immer aktuellen Software-Support unterstützen. Die Bedrohungen, denen Sie ausgesetzt sind, entwickeln sich tagtäglich weiter. Daher ist die richtige Sicherheitsstrategie ausschlaggebend, um Ihre Chancen gegen diese Bedrohungen zu erhöhen.

RECHTSSTELLUNG:
© Copyright 2018 HP Development Company, L.P. Änderungen ohne Vorankündigung vorbehalten. Die einzigen Garantien für HP-Produkte und -Services sind die explizit in den Garantieerklärungen genannten, die im Lieferumfang dieser Produkte und Services enthalten sind. Keine Aussage in diesem Dokument kann als zusätzliche Garantieerklärung ausgelegt werden. HP haftet nicht für technische bzw. redaktionelle Fehler oder fehlende Informationen. AMD ist eine Marke von Advanced Micro Devices Inc., Google Play ist eine Marke von Google Inc., Intel und Core, Optane und vPro sind Marken der Intel Corporation in den USA und/oder anderen Ländern. Microsoft und Windows sind in den USA und/oder anderen Ländern eingetragene Marken der Microsoft Corporation.

Microsoft und Windows sind in den USA und/oder anderen Ländern eingetragene Marken der Microsoft Corporation. Nicht alle Funktionen stehen in allen Ausgaben oder Versionen von Windows zur Verfügung. Um Windows-Funktionen in vollem Umfang nutzen zu können, sind unter Umständen ein Hardware-Upgrade und/oder zusätzliche Hardware, Treiber, ein BIOS-Update und/oder Software erforderlich. Windows 10 wird automatisch aktualisiert. Diese Funktion ist immer aktiviert. Für Updates können Datengebühren des Internetdienstanbieters anfallen. Die Update-Voraussetzungen können sich mit der Zeit ändern. Siehe http://www.windows.com.

Wi-Fi® ist eine Marke der Wi-Fi® Alliance.

VIELEN DANK.

Weitere Informationen finden Sie auf:
ww.hp.com/go/windows10now

Windows 10 Pro

Sorgen Sie für einen besseren Rund-um-Schutz.