Whitepaper Internet Security von A bis Z

Inhaltsverzeichnis

1 Einleitung

In der modernen Informations- und Kommunikationstechnologie spielt die die IT-Sicherheit heutzutage eine wichtige Rolle, welche man nicht unterschätzen sollte.

Der Schutz von wichtigen Daten und die Sicherheit im Cyberraum werden immer wichtiger. Des Weiteren bauen Organisationen und Unternehmen ihre Digitalen Dienstleistungen immer weiter aus. Ins besonders angetrieben wurde die ohnehin schnell fortschreitende Digitalisierung durch die Coronapandemie. Dabei wurde die Kommunikation und Zusammenarbeit zwischen Unternehmen, Privatpersonen, SchülerInnen und Schülern und in vielen anderen Bereichen weiter digitalisiert. Dies ist auch den Leuten nicht entgangen, die daraus unrechtmäßig Profit schlagen wollen. Dem Entsprechend nimmt die Cyberkriminalität in den letzten Jahren stark zu. Die Angreifer werden dabei immer kreativer und passen sich den aktuellen Sicherheitsstandards und Umständen rasch an.

Dabei wird der breiten Masse oft von den Medien ein falsches Bild von Viren und Malware vermittelt, welche solche Angriffe häufig als blinkende Bildschirme mit Duzenden Alarm-Meldungen zeigen. Doch die Realität sieht dabei ganz anders aus. Die Angriffe spielen sich meistens unbemerkt im Hintergrund ab und ohne Schutzsoftware merkt man sie erst wenn es schon zu spät ist. Sie zielen üblicherweise dabei hauptsächlich darauf ab, so viel Geld wie möglich zu erbeuten und nicht Chaos zu verbreiten. Ein moderner Virus verschlüsselt beispielsweiße alle Daten eines Unternehmens und verlangt anschließend ein Lösegeld, um diese wieder zu entschlüsseln.

Zum Beispiel kann ein Virus einen Keylogger auf Ihrem Gerät installieren, welcher darauf abzielt Kontodetails und Passwörter des Users zu speichern und an den Hacker weiterzuleiten. Damit versucht der Angreifer anschließend sich beispielsweiße in das Bankkonto des Betroffenen einzuloggen und dieses zu plündern.

Doch wie sieht die Zukunft aus? Die zukünftigen Entwicklungen der Sicherheitsbedrohungen sind schwer vorherzusagen. Vor einigen Jahren hieß es noch, dass es niemals mehr als einige Hundert verschiedene Viren gibt und Bill Gates behauptete, dass im Jahr 2006 Spam kein Problem mehr darstellen wird. Dennoch gibt es heute viel mehr als nur 100 verschiedene Viren und das Spam immer noch ein Problem ist weiß jeder, der ein E-Mail-Postfach für einige Zeit hat. Niemand weiß genau was die Zukunft mit sich bringen wird. Sicher ist nur, dass es immer Kriminelle geben wird, die versuchen, aus Angriffen und Sicherheitslücken Profit zu schlagen.

2 Worauf Sie achten müssen von A bis Z

2.1 Advanced Persistent Threat (APT)

Wenn sich eine unautorisierte Person bei einem Angriff Zugriff auf ein Netzwerk verschafft und sich in diesem möglichst lange unbemerkt aufhält, so spricht man von einem sogenannten Advanced Persistent Threat (APT). Das Ziel eines solchen Angriffs ist es in erster Linie, Daten zu stehlen aber keine bemerkbaren Schäden anzurichten. Ziel solcher Angriffe sind häufig Organisationen, bei welchen wertvolle Informationen zu erbeuten sind. Dazu gehören häufig Finanzdienstleister oder Ministerien.

2.2 Adware

Adware ist, wie der Name schon sagt, eine Software, welche Werbung auf Ihren Computer einblendet (Ad = englisch für Werbung). Diese Werbung kann in Form von Webebannern oder Pop-up-Fenstern sowohl während Sie eine Website besuchen als auch wenn Sie eine Anwendung nutzen, angezeigt werden. Werbung muss jedoch nicht immer schlecht sein, denn diese kann beispielsweise die Entwicklung von der Software finanzieren, die Sie nutzen, und es den ermöglicht den Entwicklern Inhalte kostenlos zur Verfügung zu stellen.

Adware kann jedoch in folgenden Fällen ein Problem darstellen:

- Wenn sie ohne Zustimmung auf Ihrem Gerät installiert wurde
- Wenn sie anwendungsübergreifend Werbung anzeigt und nicht ausschließlich in dem Programm, mit der sie geliefert wurde.
- Wenn sie ihren Browser übernimmt, um mehr Werbung zu zeigen (Browser-Hijacking)
- Wenn sie ohne ihr Einverständnis Daten zu Ihrem Surfverhalten sammelt und an Dritte weitergibt (Spyware)
- Wenn sie nur kompliziert wieder deinstalliert werden kann

2.3 Anonymisierender Proxyserver

Anonymisierende Proxyserver helfen dem Nutzer, seine Webaktivitäten zu verbergen. Mit Hilfe dieser Proxyserver kann er Webfilter umgehen und auf gesperrte Seiten zugreifen.

Für Unternehmen verursacht das kritische Sicherheits- und Haftungsrisiken:

Sicherheit: Das Umgehen der vorgesehenen Sicherheitsmaßnahmen und der Zugriff auf unzulässige Seiten stellen ein erhebliches Risiko da.

Haftung: Für Unternehmen kann es ein ernstzunehmendes Problem darstellen, da diese haftbar gemacht werden können, wenn Computer zum Anzeigen von extremistischen oder pornografischen Inhalten genutzt werden. Des Weiteren drohen Konsequenzen, wenn User durch illegale Downloads die Rechte Dritter verletzen.

2.4 Automatische Sperre

Werden Ihre Computer automatisch gesperrt? Ein enormes Sicherheitsrisiko für Unternehmen sind unbeaufsichtigte Computer. Während der Kaffeepause des Portiers kann ein Angreifer unbemerkt Daten vom Computer bzw. dem Netzwerk kopieren. Verhindern lässt sich ein solches Szenario durch automatische Bildschirmsperren. Bei Inaktivität wird das Gerät automatisch gesperrt und Angreifer benötigen ein Passwort, um den Computer nutzen zu können. Wenn Sie einen Verzeichnisdienst wie Active Directory verwenden, können Sie eine automatische Bildschirmsperre zentral konfigurieren. Zusätzlich können Mitarbeiter geschult werden, den PC immer zu sperren, wenn sie den Arbeitsplatz verlassen. Dadurch kann die Zeit, die ein PC unbeaufsichtigt und entsperrt ist, minimiert werden. Auf Windows kann ein PC einfach mit der Tastenkombination WIN+L gesperrt werden.

2.5 AutoRun-Wurm

AutoRun-Würmer sind Applikationen, welche sich die AutoRun-Funktion von Windows zunutze machen. Diese werden automatisch gestartet und ausgeführt, wenn etwas an den Computer angeschlossen wird. Meistens werden sie über USB-Sticks verbreitet und befallen den Computer, sobald er angeschlossen wird. Des Weiter gibt es auch eine AutoPlay-Funktion, welche beim Starten von Medien ausgeführt wird. Microsoft hat bei neuen Betriebssystemen diese Funktion jedoch deaktiviert, wodurch in Zukunft diese Applikation eine geringere Bedrohung darstellen. Dennoch muss man bei unbekannten Datenträgern und Geräten wie USB-Sticks sehr vorsichtig sein.

2.6 Backdoor-Trojaner

Ein Backdoor-Trojaner ist oft getarnt als seriöse Software. Damit soll der User dazu verleitet werden, die Software und den darin enthaltenen Trojaner zu starten. Es ist oft schon ausreichenden den Link einer Spam-E-Mail zu drücken, um sich einen Trojaner einzufangen.

Wird der Trojaner ausgeführt, fügt er sich zu den Autostart Programmen des Computers hinzu. Sobald der Computer also eingeschaltet wird, kann die Person dahinter, verschiedenste Dinge tun. Beispielsweise kann er Programme ausführen, auf persönliche Daten zugreifen, ändern oder neue Daten und Software (z.B. weitere Malware) hochladen.

Die derzeit bekanntesten Backdoor-Trojaner lauten Netbus, OptixPro, Subseven, BackOrifice und seit neuestem auch Zbot und ZeuS.

Um einer Infizierung mit Backdoor-Trojanern aus dem Weg zu gehen, sollte Ihr Betriebssystem und Ihre Programme (besonders Browser, da diese großes ein Einfallstor darstellen) stehts auf dem neuesten Stand sein, um Sicherheitslücken im System vorzubeugen.

2.7 Bootsektor-Malware

Ein Computer startet immer, indem er sich das Betriebssystem aus dem Bootsektor sucht und anschließend hochfährt. Eine Bootsektor-Malware ersetzt jedoch den ursprünglichen Startpfad mit einer abgeänderten infizierten Bootversion und verbirgt die ursprüngliche Datei.

Beim nächsten Systemstart wird die infizierte Software gebootet und aktiviert somit die Malware vor dem Betriebssystem. Dadurch Bootsektor Malware kann häufig auch einen Virenschutz täuschen, da dieser, üblicherweise nach dem Betriebssystem startet und damit nach der Malware, wodurch die Malware den Virenschutz falsche Informationen liefern kann. Diese Art von Malware kann durch ihren Start vor dem Betriebssystem außerdem viele Schutzmechanismen im Betriebssystem und Programmen aushebeln, da diesen eine falsche Realität vorgespielt werden kann.

2.8 Backups

Wie gut sind Ihre Backups? Mit Sicherheit haben Sie automatische Sicherungssysteme, um alle wichtigen Firmendaten im Falle eines Schadens am Server weiterhin verfügbar zu haben. Doch heutzutage sind Hardware-Schäden nicht mehr die größte Gefahr für Datenverlust, sondern Cyberkriminelle. Diese verschlüsseln Ihre Daten und verlangen Lösegeld für die Freigabe ebendieser. Damit Sie nicht auf eine Sicherung zurückgreifen und die Lösegeldforderung ignorieren werden, sind die Sicherungen das erste Ziel der Verschlüsselungssoftware. Das passiert still und heimlich, damit Sie nicht darauf reagieren können.

Daher ist es essenziell, dass Ihre Mitarbeiter und Mitarbeiterinnen keinen Zugriff auf Sicherungslaufwerke haben. Auch die Administratoren dürfen darauf keinen Zugriff haben. Legen Sie stattdessen ein eigenes Benutzerkonto an, welches als einziger Zugriff erhält. Diese einfache Maßnahme hilft der bösartigen Verschlüsselung von Sicherungsdateien vorzubeugen, da Angreifer nun mit den Konten aktiver Benutzer (die durch Angriffe wie Social Engineering, Phishing, etc. vergleichsweise einfacher zu erhalten sind) nicht die Backups angreifen und verschlüsseln können.

Entscheidend für eine gute Backup-Strategie ist nicht nur die Regelmäßigkeit von Sicherungen, sondern auch die Art von Sicherungen. Überlegen Sie sich daher, auf welche Art und Weise Sicherungen erstellt werden, denn die Dauer einer Wiederherstellung kann stark variieren. Wenn Sie nur die Dateien sichern, aber das Serversystem ungesichert lassen, müssen Ihre Informatiker und Informatikerinnen zuerst einen passenden Server installieren um anschließend die Daten wieder aufzuspielen. Das setzt voraus, dass die ganze Konfiguration dokumentiert ist. Einfacher ist es ein System vollständig inklusive Konfiguration zu sichern, denn dann braucht nur das Backup wiederhergestellt werden und Sie haben dieselbe Konfiguration wie zuvor. Das reduziert die Wiederherstellungszeit beträchtlich, benötigt aber mehr Kapazität. Windows bietet mit dem Programm "Server Sicherung" bereits ein kostenloses Programm, um Ihr System vollständig zu sichern. Auch für andere Systeme gibt es entsprechende Lösungen - nutzen Sie diese.

2.9 Benutzerkonten

Kennen Sie den richtigen Umgang mit Benutzerkonten? Teilen Sie niemals Benutzerkonten, sondern vergeben Sie für jeden Mitarbeiter und jede Mitarbeiterin ein eigenes Konto. Keines dieser Konten sollte über Administrator-Rechte verfügen, auch nicht die persönlichen Konten von IT-Mitarbeitern. Administrator-Rechte sollten nur spezielle Konten haben, welche im täglichen Betrieb nicht eingesetzt werden. So verhindern Sie eine sogenannte Rechte-Eskalation, bei der die Schadsoftware die Rechte des angemeldeten Benutzers übernimmt. Schadsoftware mit Administratorrechten hat vollständige Kontrolle über das Gerät, oder, je nach Berechtigungen des Administrators, das ganze Netzwerk. Für die einfache Verwaltung von Benutzerkonten bieten sich Verzeichnisdienste wie Microsoft Active Directory an. Damit können Sie zentral alle Rechte verwalten.

Beim Ausscheiden von Mitarbeitern müssen den Konten dieser Mitarbeiter die Rechte entzogen werden. Dafür empfehlen wir eine Checkliste anzulegen, die sowohl beim Anlegen als auch beim Sperren von Benutzerkonten zur Anwendung kommt. Damit wird das Risiko, Konten zu vergessen, reduziert. Einige Programme erlauben es auch, externe Authentifizierung (Single-Sign on) zu nutzen. Diese Option erlaubt es beispielsweise, User via Active Directory (LDAP) zu authentifizieren und reduziert damit die Anzahl der Accounts, die jeder User hat. Das reduziert direkt die Anzahl der Passwörter, die sich ein User merken muss und den administrativen Aufwand beim Accountmanagement.

Strikt getrennte Benutzerkonnten ermöglichen es auch, einem Mitarbeiter, der die Firma verlässt, zuverlässig den Zugriff zu sperren. Wenn sich dieser Mitarbeiter aber mit einem oder mehreren immer noch aktiven Mitarbeitern ein Konto teilt, kann es leicht sein, dass bei einem der geteilten Konten das Passwort nicht zurückgesetzt wird, und der Mitarbeiter dann immer noch Zugriff auf interne Firmengeheimnisse hat.

2.10 Betroffenenanfragen

Wissen Ihre Mitarbeiter und Mitarbeiterinnen, wie diese mit Betroffenenanfragen laut DSGVO umgehen müssen? Das Ignorieren oder nicht beantworten von Anfragen kann zu Geldstrafen führen, daher sollten diese niemals ignoriert werden. Um eine Anfrage gesetzeskonform zu beantworten, sollten Sie zudem wissen, wo welche Daten gespeichert werden. Hierfür schreibt der Gesetzgeber ein sogenanntes Verfahrensverzeichnis vor. Dieses muss auch bei einer Kontrolle durch die Datenschutzbehörde vorgelegt werden können. Mit der Software easyGDPR können Sie ein DSGVO-konformes Verfahrensverzeichnis selbst erstellen und anpassen. easyGDPR DSAR kann außerdem die Antwort auf Betroffenenanfragen größtenteils automatisieren.

2.11 Bin ich bereits betroffen?

Kennen Sie die Website **haveibeenpwned.com**? Dort können Sie überprüfen, ob ihre Kontoinformationen bereits bei einem bekannten Datendiebstahl entwendet wurden. In den vergangenen Jahren wurden beispielsweise Millionen von Nutzerdaten von Diensten wie Facebook, Dropbox, Uber, Twitch usw. gestohlen. Verwenden Sie dasselbe Passwort für mehrere Dienste, können Angreifer die gestohlenen Informationen verwenden, um andere Konten von Ihnen zu übernehmen, daher sollten Sie regelmäßig auf haveibeenpwned.com überprüfen, ob Sie bereits Opfer eines Datendiebstahls geworden sind. Der Dienst ist kostenlos und genießt hohe Reputation. Verschiedene Passwörter für verschiedene Accounts zu nutzen wäre eine noch bessere Lösung, da ein Datendiebstahl damit nur einen Account betreffen kann. Dazu muss noch gesagt werden, dass kleine Abwandlungen am Passwort kaum einen Schutz bieten. Verschiedene Passwörter müssen tatsächlich vollständig verschieden voneinander sein. Ein Passwortmanager hilft dabei, eine Vielzahl an wirklich verschiedene Passwörter zu verwalten.

2.12 Botnet

Sobald ein Computer mit einer Botnet-Schadsoftware infiziert ist, kann der Angreifer das Gerät über das Internet steuern. Ab diesem Zeitpunkt folgt der Computer nur noch den Befehlen des Hackers, während der Benutzer nichts davon merkt. Werden mehrere infizierte PCs gleichzeitig kontrolliert, so spricht man von einem Botnet. Die Botnets werden meistens genutzt um Distributed-Denial-of-Service-Angriffe (DDoS) durchzuführen. Dabei greifen Tausende Computer gleichzeitig auf eine Website oder ein System zu und legen diese dadurch lahm. Botnets können allerdings auch als Spyware zum Datendiebstahl, oder für eine Vielzahl von anderen illegalen Aktivitäten genutzt werden.

2.13 Browser-Hijacker

Nachdem Ihr Computer oder Browser von einem Hijacker übernommen wurde, können Sie unter Umständen die Startseite Ihres Browsers nicht mehr ändern. Dabei bearbeiten die Hacker die Windows-Registry, so dass bei jedem Neustart des PC die gesetzten Einstellungen wiederhergestellt werden. Ein Hacker kann mit einem übernommenen Browser zusätzliche Malware installieren, den Inhalt von besuchten Seiten (wie auch Online-Banking, …) lesen, den User ohne das er oder sie etwas merkt auf gefälschte Phishing-Seiten umleiten um Zugangsdaten und persönliche Informationen abzugreifen und vieles mehr.

2.14 Brute-Force-Angriff

Ein Brute-Force-Angriff wird häufig eingesetzt, um an Passwörter zu gelangen. Die Angreifer verwenden dabei spezielle Software um automatisiert eine Vielzahl verschiedener Passwörter zu probieren.

Am besten schützen Sie sich gegen derartige Angriffe mit einem möglichst komplexen, aber vor Allem langen Passwort. Jedes zusätzliche Zeichen, das ein Passwort besitzt, erschwert einen Brute-Force Angriff auf das Passwort um ein Vielfaches.

2.15 Buffer Overflow (Pufferüberlauf)

Wenn ein Programm mit mehr Daten konfrontiert wird, als es verarbeiten kann, so spricht man von einem Pufferüberlauf. Wenn das passiert, geht dem System der Speicherplatz aus und es kann dazu kommen, dass es versehentlich Teile des Speichers außerhalb des dem Programm zugeordneten Speichers überschreibt. Buffer Overflow Angriffe machen sich diese Schwäche zu nutzen, um nicht autorisierten Code auszuführen, Informationen aus dem Innenleben anderer Programme auszulesen oder gleich das ganze System lahmzulegen.

2.16 Command and Control Center

Das Command and Control Center (oder auch Command and Control Server, C&C) ist ein PC oder Server, welcher ein Botnet steuert. Durch das C&C können Hacker Anweisungen an ihr Botnet verteilen und

Daten abholen. Häufig werden diese Botnets für Denial-of-Service-Angriffe eingesetzt, da so tausende von Computern gleichzeitig auf dieselbe Website zugreifen können und diese vollständig blockieren können. Sie können aber auch für andere Malwareangriffe genutzt werden, etwa um Daten zu stehlen.

2.17 Cookies

Jede Website, die man beim Surfen im Internet aufruft, kann auf Ihrem Computer kleine Dateien, die auch „Cookies“ genannt werden, hinterlassen. Diese Cookies sind besonders dafür bekannt, User überall im Internet zu verfolgen, persönliche Daten zu sammeln und diese entweder direkt oder in Form von „Targeted Ads“ zu verkaufen. Dadurch verletzen diese Cookies ihre Privatsphäre, aber beschädigen nicht Ihren Computer. Cookies können aber viel mehr. Ursprünglich wurden Cookies entwickelt, um Einstellungen wie Ihr Warenkorb in einem Onlineshop oder die Cookie Einstellungen selbst, sowie Anmeldedaten zu speichern, damit Sie beim nächsten Besuch nicht alles neu einrichten müssen.

Alle Cookies, die gesetzt werden, dürfen nur von der Website gelesen werden, die das Cookie gesetzt hat. Das bedeutet, dass ein Cookie das von z.B. schindler-it.com gesetzt wird, nicht von anderen Websites gelesen werden kann. Damit sollte eine Verfolgung über Cookies quer durch das Internet nicht möglich sein, doch Trackingplattformen haben einen Weg um das Problem herum gefunden. Indem die Website, die sie besuchen, ein Skript (Programmcode) von einer Trackingplattform einbindet, kann dieses Skript Cookies für die Website der Trackingplattform setzen, von der das Skript kommt. Damit kann die Trackingplattform, die ja die eigenen Cookies lesen kann, die Informationen von verschiedenen Websites, die das Skript derselben Trackingplattform eingebunden haben, sammeln, lesen und auswerten. Um Tracking durch Cookies (welches nur eine von vielen Formen von Tracking ist) zu umgehen können verschiedene Mittel eingesetzt werden. Browser wie Firefox sind mehr privatsphärenfokussiert als z.B. Chrome und bieten teilweise, wie im Fall von Firefox, einen eingebauten Adblocker an. Alternativ können Sie einen Adblocker als Extension hinzufügen. Des Weiteren können Sie Ihren Browser so einstellen, dass er „seitenübergreifende Cookies“ blockiert. Wie vorher erwähnt nutzen Trackingplattformen Cookies die von einem Skript einer anderen Website (der Website der Trackingplattform) statt der Seite, die sie besuchen, gesetzt werden. Diese Cookies werden damit blockiert. Dieser Ansatz hat allerdings auch Nachteile. Während die meisten Websites problemlos funktionieren, wenn man seitenübergreifende Cookies blockiert, können manche Websites dadurch den Dienst quittieren. In diesem Fall kann man diese Websites zu den Ausnahmen des Cookieblockers in Ihren Browsereinstellungen hinzufügen, um die Funktionalität wiederherzustellen.

2.18 Datendiebstahl

Von Datendiebstahl spricht man, sobald Daten gezielt gestohlen werden. Dieser kann aber nicht nur von kriminellen Hacker vollzogen werden. Es kann auch ein verärgertes Familienmitglied oder Mitarbeiter einer Firma sein. Hacker setzten meist Malware wie zum Beispiel Trojaner oder Keylogger ein, um an sensible Daten zu kommen. Um das Risiko und den Schaden den ein Datendiebstahl durch unternehmensinterne Personen anrichten kann zu reduzieren, sollten alle Personen nur Zugriff auf die Informationen, die sie für Ihre Arbeit benötigen, haben.

2.19 Datenleck

Die unbefugte Offenlegung von Daten bezeichnet man als Datenleck. Passiert diese Offenlegung absichtlich so spricht man von einem Datendiebstahl oder unabsichtlich von einem Datenverlust.

Das verhindern von solchen Datenlecks hat für Unternehmen oberste Priorität. Mit Hilfe von Verschlüsselungen, Virenschutzsoftware, Firewalls, Zugriffskontrolle, schriftlich festgehaltene Richtlinien und Schulungen für Mitarbeiter können diese verhindert werden. Hier wäre noch zu erwähnen, das

Homeoffice ein Schwachpunkt für Datenlecks sein kann. Firmeninformationen können sich dadurch auf Geräten und in Räumlichkeiten befinden, die Privat von Mitarbeitern genutzt werden, und dadurch für unternehmensfremde Personen zugänglich sein können. Mitarbeiter müssen daher vor der Einführung von Homeoffice ausreichend geschult werden, Firmeninformationen adäquat auch bei sich zuhause zu schützen.

2.20 Datenverlust

Von einem Datenverlust spricht man, sobald Daten versehentlich abhandenkommen oder geleaked werden. Dies geschieht meist, wenn das Gerät, auf dem die Daten gespeichert wurden, verloren geht und in möglicherweise in falsche Hände gerät. Eine gute Verschlüsselung kann in solch einem Fall schon sehr wirksam sein. Nicht mehr benötigte Datenträger und Geräte müssen ordnungsgemäß gelöscht und entsorgt werden.

2.21 Datensicherung

Wie sichern Sie Ihre Daten? Das wichtigste Kapital von Unternehmen sind im digitalen Zeitalter die Daten. Daher müssen diese optimal geschützt werden. Eine ständige Sicherung der Daten auf andere Datenträger ist inzwischen selbstverständlich. Dabei denken viele Unternehmen an einen Festplatten-Fehler und unterschätzen die Gefahr von Einbruch oder Brandschäden. Daher sollten Sie mindestens einen Sicherungsdatenträger an einem physisch anderen Standort aufbewahren. Sicherungen können z.B. in die Cloud (Dropbox, OneDrive) übertragen werden oder Sie setzen auf Wechseldatenträger, welche regelmäßig ausgetauscht werden.

2.22 Datenträgerausmusterung

Wissen Sie was mit Ihren Datenträgern passiert, wenn Sie diese aus dem Unternehmen ausmustern? In den meisten Fällen ist die Antwort nein, deshalb sollten Sie sicherstellen, dass alle Daten vollständig gelöscht wurden. Löschen Sie eine Datei auf Ihrem Computer, dann wird diese in Wirklichkeit nicht gelöscht. Das System „vergisst“ nur, wo auf der Festplatte die Datei gespeichert ist. TechnikerInnen können die Dateien weiterhin sehr einfach wiederherstellen. Für zuverlässiges Löschen sollte daher die Festplatte daher vollständig formatiert werden. Dieser Vorgang dauert mehrere Stunden, überschreibt aber jede Speicherzelle auf dem Datenträger. Achten Sie darauf, dass die häufige angebotene Option "Schnellformatierung" nicht ausreichend ist. Alternativ können Sie alte Datenträger auch professionell vernichten lassen.

2.23 Datenverschlüsselung

Verschlüsseln Sie Ihre Daten? Bei Diebstahl oder Verlust von Firmen-Computern als auch beim Einbruch in das Firmengebäude besteht die Gefahr von Datendiebstahl. Sollte sich ein solcher Vorfall ereignen, sind Sie verpflichtet eine Meldung bei der österreichischen Datenschutzbehörde durchzuführen. Je nach Art der gestohlenen Daten kommen Sie mit einer Verwarnung davon oder müssen eine Geldstrafe (bis zu 4% des Jahresumsatzes sind möglich) entrichten. Dabei lässt sich Datendiebstahl leicht verhindern, indem Sie Datenträger verschlüsseln. In diesem Fall sind die entwendeten Daten für Unbefugte nicht lesbar. Die Einrichtung einer Festplattenverschlüsselung ist einfach und fällt im laufenden Betrieb auch nicht mehr auf. Bei Computern mit Windows Betriebssystem können Sie einfach die integrierte Festplattenverschlüsselung "Bitlocker" einsetzen (verfügbar nur in Professional und Enterprise-Editionen). Für die Benutzer entsteht im täglichen Betrieb kein zusätzlicher Aufwand.

2.24 Denial-of-Service-Angriff

Bei einem Denial-of-Service-Angriff werden Benutzer daran gehindert, eine Website aufzurufen oder auf einen Computer zuzugreifen. Bei einem DoS-Angriff werden keine Daten beschädigt oder gestohlen, Sie sorgen lediglich dafür das Webserver nicht erreichbar sind. Doch auch diese Dienstunterbrechung kann für den Betroffenen sehr kostspielig sein.

Denial of Service Angriffe können mithilfe von Botnets stark skaliert werden. Diese Angriffe werden dann Distributed Denial of Service (DDos) Angriffe genannt.

2.25 DNS-Hijacking

Das DNS-Hijacking ist eine Angriffsmethode, welche Ihren Datenverkehr auf gefälschte Websites weiterleiten oder alternative Inhalte anzeigen kann. Meistens werden diese verwendet, um private Daten und Zugangsdaten zu stehlen

2.26 Dokument-Malware

Dokument-Malware sind schädliche Inhalte, die von den Angreifern in Dokumente eingebettet werden. Sobald der nichtsahnende User das Dokument öffnet, wird versteckte Malware ausgeführt. Meisten befinden sich diese Dateien in Excel-, Word- und PDF-Dokumenten.

2.27 Drive-by-Download

Ein sogenannter Drive-by-Download geschieht unbemerkt im Hintergrund. Dabei reicht meist das Aufrufen einer Infizierten Website aus, um den Download der Malware zu starten. Dabei nutzt der Angreifer Sicherheitslücken im Browser des Users, um den PC zu infizieren.

Jeden Tag werden seriöse Websites von Hackern manipuliert und mit schädlichem Code ergänzt. Ruft der User anschließend die Website auf, startet der Drive-by-Angriff automatisch im Hintergrund. Damit man sich vor dieser Art von Angriff schützen kann, sollte man die aktuelle Version des Browsers und eine aktuelle Browser Endpoint-Sicherheitssoftware verwenden, welche mit Webschutzfiltern ausgerüstet ist.

2.28 E-Mails als Angriffspunkt

Emails sind eines der wichtigsten Kommunikationswege in Unternehmen, gleichzeitig aber auch der beliebteste Angriffskanal von Cyberkriminellen. Mit künstlicher Intelligenz erzeugen diese bereits heute gefälschte Emails, die nicht mehr vom Original zu unterscheiden sind. Im Anhang befindet sich oftmals eine Excel- oder Worddatei. Diese wurde mit Makro-Funktionen ergänzt, die automatisch Schadsoftware installieren und ausführen. Ein einfacher Weg diese Angriffe zu minimieren ist das automatische Ablehnen von Emails mit entsprechendem Anhang. Word-Dokumente mit Makros werden als .docm abgespeichert, während "normale" Word-Dokumente als .docx abgelegt werden. Bei Excel ist die Dateiendung .xlsm. Wenn Sie diese beiden Dateianhänge automatisch ablehnen haben Sie einen ersten Schritt gesetzt, um das Risiko einer Cyberattacke zu minimieren. Komplexere Angriffe über Emailanhänge können mit einer Firewall mit eingebautem E-Mail-Schutz und einem guten Virenschutz auf dem Endgerät blockiert werden. Eine Firewall mit sogenannter Sandbox-Technologie kann jeden Anhang auf gefährliche Funktionen prüfen, bevor der User überhaupt die Möglichkeit hat die Malware versehentlich zu aktivieren.

2.29 E-Mail-Spoofing

Beim E-Mail-Spoofing wird die Absenderadresse gefälscht. Auf diese Art und Weise täuschen die Angreifer vor, dass die E-Mail etwa von Ihrer Bank gesendet wurde. Anschließend werden Sie auf eine gefälschte Website weitergeleitet, welche Sie nach Ihren Kontodetails fragt. Außerdem verdecken die Kriminellen durch die gefälschten E-Mail-Adressen Ihre Spuren und machen eine Nachverfolgung beinahe unmöglich.

2.30 Exploit

Ein Exploit nutzt bekannte Sicherheitslücken in einem System aus, um auf einen PC zugreifen zu können und diesen zu infizieren. Jedoch wird dieser wirkungslos, wenn die Lücke mittels Patch oder Update geschlossen wird.

Von sogenannten Zero-Day-Exploits spricht man, wenn Hacker die gefunden Lücken rasch nutzen, bevor die Entwickler die Sicherheitslücke schließen können. Damit Sie optimal vor Exploits geschützt sind, sollten Sie stehts darauf achten, dass Ihr Virenschutz- oder Endpoint-Sicherheitssoftware aktiviert und auf dem neuesten Stand ist.

2.31 Firewall ausreichend?

Ist eine Firewall ausreichend, um ein Netzwerk zuverlässig zu schützen? Nein, denn nicht alle Angriffe haben im Internet ihren Ursprung. Besonders gefährdet sind Sie, wenn Sie alle Computer, Drucker, Server und Backup-Systeme im selben Netzwerk betreiben. Denn dann können Trojaner und Viren alle Systeme befallen, ohne dass die Firewall schützend eingreifen kann. Daher sollten Sie Ihr System in verschiedenen Netzen unterteilen. Haben Sie ein eigenes Netz für Ihre Sicherungssysteme, dann erfolgt jeder Zugriff über die Firewall, welche etwaige Angriffe abwehren kann. So verhindern Sie, dass Infektionen einzelner Computer das gesamte Netzwerk infizieren. Stattdessen können Sie die befallenen Geräte isolieren ohne, dass die gesamte Firma währenddessen stillsteht.

Damit das Homeoffice nicht zur Sicherheitslücke wird beachten Sie bitte folgende Hinweise: Zugriffe auf das Firmen-Netz sollte nur über gesicherte Verbindungen möglich sein. Damit MitarbeiterInnen auf das Arbeitsgerät zugreifen können nutzen Sie entweder eine VPN-Lösung oder setzen Sie TeamViewer (Lizenzierung beachten!) ein. Weiters sollten keine Privatcomputer für den Homeoffice Betrieb eingesetzt werden. Die eingesetzten Betriebsgeräte sollten zudem verschlüsselt werden. Vereinbaren Sie zudem mit Ihren Mitarbeitern fixe Regeln für den Umgang mit Firmendaten im Privathaushalt, z.B. das Absperren des Arbeitszimmers bzw. Wegsperren von Akten.

2.32 Gefälschter Virenschutz

Wie der Name schon sagt, gibt es auch unter den Programmen, die dich schützen sollen, schwarze Schafe. Sie geben sich fälschlicherweise als Virenschutz aus und melden nicht existente Bedrohungen.

Ihr Ziel ist es dabei den Benutzer zu verunsichern und Ihn dazu verleiten Geld für ein Produkt auszugeben, welches das Problem angeblich beheben soll. Ein gefälschter Virenschutz wird auch als Scareware bezeichnet. Installiert wird er meistens über schädliche Websites, zu denen die Opfer meist mittels Spam-Nachrichten gelangen. Das Ziel ist auch hier den Opfern möglichst viel Geld aus der Tasche zu ziehen.

2.33 Hacktivismus

Hackeraktivitäten mit gesellschaftlichem oder politischem Hintergrund werden als Hacktivismus bezeichnet und zielen meist auf Regierungen, Organisationen oder Einzelpersonen ab. Solche Hacktivisten verunstalten Websites, starten DoS-Angriffe oder stehlen Daten, um auf sich aufmerksam zu machen und Ihre Meinung zu verbreiten.

2.34 Hoax

Als Hoaxes bezeichnet man Falschmeldungen, um Nutzer zu täuschen oder zu betrügen. Ziel ist auch hierbei meistens Geld zu machen, Bandbreite zu verbrauchen oder Malware zu installieren.

Am häufigsten behaupten Hoaxes die folgenden Dinge:

- Sie warnen vor nicht existenter, höchst schädlicher Malware.
- Sie behaupten E-Mails mit einem bestimmten Betreff enthalten Malware.
- Sie geben vor Warnungen von großen Softwareunternehmen, Regierungen oder Internetdienstanbieter zu sein.
- Sie behaupten, dass ein Virus unmögliche Dinge tut.
- Sie fordert Sie auf, die Warnungen weiterzuleiten

Am besten schützen Sie sich gegen solche Falschmeldungen, indem Sie sich über solche Gefahren informieren und eventuell online Nachforschungen über aktuelle oder vergangene Hoaxes betreiben.

2.35 HomeOffice

Wurden Sie auch von der Corona-Krise überrascht und mussten über Nacht zig Mitarbeiter in den HomeOffice Betrieb senden? Hoffentlich haben Sie dabei auf die Cybersecurity geachtet und Ihr Firmennetzwerk nicht Gefahren ausgesetzt. Firmeninterne Server sollten nicht direkt aus dem Internet kontaktiert werden können. Der Fernzugriff auf diese Server und den Rest des Firmennetzwerks sollte immer über eine VPN-Verbindung durchgeführt werden. Dabei muss sich jeder Benutzer und jede Benutzerin vorab authentifizieren. So haben nur berechtigte Personen Zugriff auf die Firmen-Ressourcen. Der Datenverkehr wird dabei automatisch verschlüsselt. Wenn Ihre Firewall eine solche Funktion nicht bietet oder Sie noch keine Business-Firewall besitzen, ist es höchste Zeit Ihr Netzwerk mit damit zu ergänzen.

2.36 Honeypot

Honeypots stellen keine Bedrohung für den normalen Nutzer da. Als Honeypot wird ein Gerät, Account oder andere Ressource bezeichnet, die nicht im Aktiven Betrieb genutzt wird, aber für Hacker interessant aussieht. Dieser Honeypot wird genau überwacht um versuchte Zugriffe, die im Normalbetrieb des Unternehmens nicht vorkommen, zu entdecken. Damit können sie versuchte Angriffe oder Angriffe, die noch keinen oder minimalen Schaden anrichten konnten, entdecken. Sicherheitsforscher nutze Honeypots außerdem zu Forschungszwecken, indem sie Honeypots absichtlich infizieren lassen und dann beobachten was die Schadsoftware macht.

2.37 Internetwurm

Unter Internetwürmern bezeichnet man Malware, welche sich selbst kopiert und verbreitet. Dabei spielt es keine Rolle, ob es in lokalen Netzwerken oder online geschieht.

Die Tatsache das Würmer sich selbst verbreiten können und keine Programme oder Dateien dafür benötigen, ist der Unterschied zu herkömmlichen Viren. Sie nutzen dabei die Kommunikation zwischen den Geräten, um sich zu verbreiten.

Es gibt aber auch sogenannte Wurm Conficker, welche Sicherheitslückens ausnutzen, um Computer zu infizieren. Andere hingegen sind dazu da, um den Hacker Zugang zu einem PC zu verschaffen und damit auch die Kontrolle über das Gerät.

2.38 Keylogging

Ein Keylogger zeichnet die Tastatureingaben des Users im Hintergrund auf und gibt diese an Dritte weiter. Ziel ist es dabei Passwörter, Benutzernamen, Kreditkartendaten oder Ähnliches zu stehlen.

2.39 Malware

Der Begriff Malware ist die allgemeine Bezeichnung für jegliche Art von Schadsoftware. Unter diesen Begriff fallen zum Beispiel Viren, Trojaner, Würmer und Spyware.

2.40 Mobile Malware

Bei einer Mobile Malware handelt es sich um eine speziell für Smartphones entwickelte Schadsoftware. Mobile Malware verbeitet sich seit 2010, als man erste mobile Geräte identifizierte, welcher von einer Malware befallen wurden. Besonders Android Geräte sind davon stärker betroffen als IOS. Das liegt primär daran, dass Apps aus nicht vertrauenswürdigen Quellen viel leichter auf Android installiert werden können als auf IOS. Ein Virenschutz für Mobilgeräte, sowie Vorsicht bei der Installation von Apps ist heutzutage wichtiger denn je zuvor.

2.41 Office Makros

Wissen Sie was Office Makros sind bzw. verwenden Sie diese Funktion? Damit können Sie in Word- oder Excel-Dokumenten programmieren. Mehr als 90% aller Benutzer nutzen diese Funktion nicht. Trotzdem rückt diese in den vergangenen Jahren immer mehr in den Fokus, denn Kriminelle nutzen diese aus, um Ihre persönlichen Daten zu verschlüsseln. Sogenannte Ransomware (deutsch: Verschlüsselungstrojaner) werden in Office-Makros versteckt und führen nach dem Aufrufen gefährliche Funktionen aus. Deaktivieren Sie daher diese Funktion dauerhaft und stellen Sie sicher, dass diese auch nicht vom Benutzer irrtümlich aktiviert werden können. Verzichten Sie zudem auf ältere Office Versionen wie Office 2010, welche in dieser Hinsicht viel weniger Sicherheitseinstellungen bieten als moderne Pakete.

2.42 Parasitenviren

Dateiviren, die sich verbreiten, indem Sie sich an Programmdateien von unschädlicher Software anhängen, bezeichnet man als Parasitenviren. Wenn ein infiziertes Programm gestartet wird, führt der Virencode seine Instruktionen aus und kann weitere Malware installieren, Daten stehlen und vieles mehr. Danach startet er und das richtige Programm und übergibt diesem die Kontrolle. Für das Betriebssystem sieht es so aus als wäre er Teil des Programmes und es vergibt daher die gleichen Rechte. Aktuelle bespiele für Parasitenviren sind Sality, Virut und Vetor.

2.43 Passwort-Manager

Ein einzigartiges Passwort für jede Website wählen und merken? Für viele Menschen ist dies aufgrund der Vielzahl an Benutzerkonten nahezu unmöglich. Daher setzen viele fälschlicherweise auf ein Passwort für alle Dienste oder ändern ein Passwort nur geringfügig ab. Wenn nun ein einziger Account kompromittiert wird, können Hacker dieses Passwort nutzen um sich bei anderen, potenziell wichtigeren Accounts wie Onlinebanking einzuloggen und viel mehr Schaden anrichten. Nur leicht abgeänderte Passwörter bieten kaum einen zusätzlichen Schutz. Daher werden möglichst komplexe, lange und einzigartige Passwörter für jeden Account benötigt. Wie soll man sich das merken? Die Antwort: Sie merken sich nur ein einziges Passwort für Ihren Passwortmanager und überlassen ihm den Rest!

Passwort Manager speichern Ihre Passwörter auf sichere Art und Weise. Um darauf zugreifen zu können müssen Sie sich mit Passwort, Fingerabdruck oder ähnlichem anmelden. So können Sie für jeden Dienst ein eigenes Passwort nutzen und müssen sich diese nicht mehr merken. Besuchen Sie eine entsprechende Website fügt der Passwortmanager die Anmeldedaten automatisch ein. Passwort gibt es sowohl in kostenloser (z.B. KeePass) als auch in kostenpflichtiger (z.B. 1Password) Ausführung. Spezialisierte

Passwortmanager wie 1Password bieten in der Regel mehr Komfortfunktionen und mehr Schutz als Programme, die einen Passwortspeicher nur als Zusatzfunktion anbieten (z.B. die „Passwort merken“ Funktion in Browsern).

2.44 Patches

Patches sind kleine Updates für Programme, um aktuelle Sicherheitslücken oder Fehler zu beheben. Es ist daher wichtig regelmäßig Patches und Updates zu installieren, um Sicherheitslücken in Ihren Programmen und Ihrem Betriebssystem so schnell wie möglich zu schließen.

2.45 Phishing-E-Mail

Phishing zielt darauf ab, vertrauliche Informationen zu erhalten und anschließend an Dritte weiterzugeben.

Dabei geben sich diese E-Mails meist als seriöse Organisation aus, wie zum Beispiel:

- Banken
- Bekannte Online-Spiele
- Soziale Netzwerke
- Online Dienste mit Zugriff auf Ihre Bankdaten
- Eine Abteilung Ihres eigenen Unternehmens

Zum Schutz vor solchen E-Mails sollte Sie in der Regel vermeiden, Links in E-Mails aufzurufen, ohne den Link vorher zu überprüfen. Die Meisten Phishing-E-Mails können mit Hilfe von einer Anti-Phishing-Software erkannt werden.

2.46 Potenziell unerwünschte Anwendung (PUA)

Sogenannte potenziell unerwünschte Anwendungen sind nicht schädlich im herkömmlichen Sinne, können jedoch aus der Sicht des Anwenders ein unerwünschtes Verhalten aufweisen oder unerwünschte Sicherheitslücken und Einfallstore für Malware öffnen. Einige Virenscanner erkennen und blockieren PUAs automatisch.

2.47 Ransomware

Ransomware versperrt Ihnen den Zugriff auf Ihre eigenen Dateien oder Computer und verschlüsselt üblicherweise Ihre Daten. Danach erpresst es Sie und fordert Sie auf ein Lösegeld zu bezahlen, um wieder an Ihre Daten zu gelangen. Gute, zuverlässige und geschützte Backups sind hier Gold wert. Ein Backup das allerdings mit den restlichen Daten mitverschlüsselt wird, hilft Ihnen auch nicht weiter. Daher sollten Sie ein Backup offline oder schreibgeschützt aufbewahren.

2.48 Rootkit

Wenn man sich eine Malware einfängt, installiert diese häufig ein Rootik, um seine Prozesse versteckt ausführen zu können. Ein Rootkit kann beispielsweise Keylogger unentdeckt im Hintergrund laufen lassen. Für moderne Endpoint-Sicherheitssysteme stellen Rootkits heutzutage meist kein Problem mehr da. Sie erkennen diese in den meisten Fällen problemlos und entfernen Sie anschließend.

2.49 Serversicherheit

Wissen Sie, ob Ihr Server sicher ist? Eventuell wird dieser täglich angegriffen und Angreifer versuchen sich unberechtigterweise auf diesem anzumelden. Daher sollten Sie zusätzlich zu anderen Sicherheitsmaßnahmen wie aktuelle Virenschutzsoftware, regelmäßige Backups und strikt konfigurierte Firewalls, fehlgeschlagene Anmeldeversuche unbedingt protokollieren. Nur so erfahren Sie, ob bereits ein Angriff stattfindet. Bei einer hohen Zahl an fehlgeschlagenen Anmeldeversuchen sollte zudem eine Warnung an

Ihr IT-Team gesendet werden, um auf den Vorfall reagieren zu können. Sie können damit außerdem IP-Adressen blockieren, die sich mehrfach versuchen unerlaubt anzumelden.

2.50 Sicherheitslücke

Unter Sicherheitslücken versteht man Fehler in Softwareprogrammen, die Hacker nutzen können, um Computer zu attackieren. Behoben werden diese Fehler durch sogenannte Patches.

2.51 Social Engineering

Als Social Engineering bezeichnet man eine Gruppe an Methoden, die psychologische Tricks nutzen, um die Menschen hinter den Bildschirmen anstelle von digitalen Sicherheitslücken auszunutzen. Social Engineering kann bei verschiedenen Angriffen von Datendiebstahl zu Phishing Angriffen bis hin zu Malwareverbreitung und vielem mehr zum Einsatz kommen. Klare Abläufe und Zuständigkeitsbereiche, sowie gut geschulte Mitarbeiter bilden eine Verteidigungslinie gegen Angriffe die Social Engineering anwenden.

2.52 Soziale Netzwerke

Soziale Netzwerke wie Facebook, Instagram oder Snapchat sind jedem bekannt und genießen weltweites Ansehen. Leider bleiben aber auch diese beliebten Plattformen von kriminellen nicht verschont. Ganz im Gegenteil: Sie werden ein immer beliebteres und attraktiveres Ziel für Hacker.

Dabei manipulieren die Angreifer häufig den Account eines Nutzers, um Schadinhalte oder Malware in Umlauf zu bringen. Daher sollten Sie sich genau überlegen, welchen Links Sie folgen und dafür sorgen, dass ihr Computer die aktuelle Antivirus Version und Patches installiert hat. Darüber hinaus sollten sie unterschiedliche sichere Passwörter verwenden und, wenn verfügbar, eine Zwei-Faktor-Authentifizierung einrichten.

2.53 Spam

Ohne Aufforderung versandte Werbe-E-Mails, also das digitale Pendant zu Werbepost im Briefkasten, bezeichnet man als Spam.

Um von Spam-Filtern nicht erkannt zu werden, tarnen die Spammer ihr E-Mail größtenteils. Die meisten Spam Mails stammen von seriösen Absendern, deren Daten gestohlen wurden und nun missbräuchlich verwendet werden.

Große E-Mail-Dienstanbieter sind häufig Opfer von Spammer, welche durch Mailware versuchen die Mail Transfer Agents (MTA) zu beschädigen. Außerdem stellt das Spamming für den Angreifer praktisch keine Kosten da, somit erzielt er bereits einen Gewinn, auch wenn nur eine Person von mehreren Tausenden einen Kauf tätigt.

2.54 Spearphishing

Gezieltes Phishing mit Hilfe von gefälschten E-Mails bezeichnet man als Spearphishing. Ziel ist es von einzelnen Mitarbeitern eines Unternehmens vertrauliche Daten und Informationen zu erhalten.

Der größte Unterschied zum herkömmlichen Phishing ist, dass beim Spearphishing E-Mails nicht ziellos und massenhaft versendet werden, sondern gezielt an bestimmte Personen gehen. Meist gibt sich der Angreifer als Mitarbeiter desselben Unternehmens aus und nutzt Social Engineering Tricks um einen vertrauenswürdigen Eindruck zu erwecken.

2.55 Spywares

Sogenannte Spyware ist eine Kategorie von Malware, die versucht Ihre Daten zu stehlen. Dieser Datendiebstahl kann verschiedene Formen annehmen. Spyware kann viele Formen von unerwünschten Trackern, die Ihre Webaktivitäten sammeln bis zu Keyloggern, die versuchen aus Ihren Tastaturanschlägen Passwörter auszulesen annehmen. Ein guter Virenschutz kann Spyware erkennen und entfernen.

2.56 SQL-Injection

Eine SQL-Injection ist ein Exploit, welcher sich die Tatsache zunutze macht, dass Software die Datenbankabfragen ausführt, nicht immer gründlich prüft, ob bei der durchgeführten Abfrage schädliche Kommandos eingeschleust wurden.

Kriminelle nutzen SQL-Injections häufig in Kombination mit Malware und Cross-Site-Scripting (XSS) um Websites zu hacken und schädlichen Code zu injizieren oder Daten zu extrahieren.

Bei einer SQL-Injection werden Befehle über HTTP-Server gesendet, welcher mit einer SQL-Datenbank verknüpft ist. Wenn jener Server nicht korrekt aufgesetzt wurde, behandelt er speziell manipulierte Daten, welche in ein Formularfeld eingefügt werden (z.B. Usernamen) als Befehle, die anschließend am Datenbankserver ausgeführt werden. Dadurch kann der Angreifer beispielsweise einen Befehl injizieren, der die komplette Datenbank ausliest. Vorsicht bei der Entwicklung von Programmen und manche Firewallfunktionen können vor dieser Art von Angriff schützen.

2.57 Teilen von Zugangsdaten

Wie teilen Sie Zugangsdaten? Es gibt verschiedene Gründe, die dazu führen, dass Zugangsdaten mit verschiedenen Mitarbeitern geteilt werden müssen. Achten Sie in diesem Fall darauf, dass das Teilen auf sichere Art und Weise durchgeführt wird. Ein Passwort per E-Mail zu senden ist ein No-Go, denn die E-Mail wird meist noch jahrelang am Server gespeichert und ist daher weiterhin zugänglich. Außerdem sind Emails nicht Ende-zu-Ende verschlüsselt, und liegen dadurch lesbar auf dem Server vor. Ein Angreifer kann nun, sobald er sich Zugang zum Server verschafft hat, diese Passwörter nutzen, um seine Kontrolle über Ihr gesamtes Netzwerk weiter auszubreiten.

Um diesem Risiko entgegenzuwirken können Sie die Funktion vieler Passwortmanager, Passwörter mit mehreren Personen zu teilen, nutzen. Gute Passwortmanager verschlüsseln Ihre Passwörter wenn Sie nicht gerade die Applikation geöffnet haben, wodurch Angreifer sie nicht einfach auslesen können.

2.58 Trojaner (Trojanisches Pferd)

Als Trojaner wird eine Malware bezeichnet, die sich als ein vertrauenswürdiges Programm ausgibt, damit der User sie ausführt.

2.59 Verdächtige Dateien

Eine sogenannte Endpoint-Protection markiert bei einem Systemcheck jede Datei: als verdächtig, schädlich oder unbedenklich. Dabei wird jede Datei auf spezielle Merkmale überprüft und anschließend dementsprechend zugeordnet. Verdächtige Dateien sind Dateien, die nicht als schädliche Programme bekannt sind, die aber einige Verhaltensmuster mit schädlichen Dateien teilen. Diese Dateien müssen überprüft und mit Vorsicht behandelt werden, da es sich bei ihnen um gefährliche Software handeln könnte.

2.60 Virus

Schädliche Computerprogramme, welche sich auf anderen Dateien ausbreiten, bezeichnet man als Viren. Eine infizierte Datei kann auf verschieden Wegen wie als E-Mail-Anhang, Download aus dem Internet oder über einen infizierten USB-Stick auf Ihren PC gelangen. Viren verstecken sich gerne in anderen Programmen oder in Code, der zum Öffnen von bestimmten Dateitypen benötigt wird.

Auch bei Viren hilft eine gute Antivirus Software und regelmäßige Updates, um Sicherheitslücken zu schließen.

2.61 Websitesicherheit

Wann haben Sie sich das letzte Mal um Ihre Website gekümmert? Achten Sie darauf, dass Ihre Homepage über ein gültiges HTTPS-Zertifikat verfügt. Nur so ist der Datenverkehr zwischen Website und Besucher verschlüsselt. Mit Lets Encrypt können Sie inzwischen kostenlose Zertifikate generieren. Der Verzicht auf diese Verschlüsselung reduziert nicht nur das Vertrauen in Ihre Website, sondern sorgt für eine schlechtere Auffindbarkeit Ihrer Homepage bei Suchmaschinen.

2.62 Wie sieht ein Hacker aus?

Sie kennen das klassische Bild von Hackern, welches die Medien transportieren? Ein junger Mann mit Kapuzenpulli sitzt in einem dunklen Raum und tippt etwas in seinen Computer, um Passwörter zu knacken. In Wirklichkeit setzen Kriminelle viel öfter auf sogenanntes Social Engineering. Dabei wird im zwischenmenschlichen Dialog versucht dem Gegenüber Geheimnisse zu entlocken, beispielsweise in dem man sich als Mitarbeiter des IT-Teams ausgibt und das Benutzerpasswort verlangt. Auch gefälschte Emails sind eine häufig angewandte Methode. Schulen Sie daher Ihre Mitarbeiter auf solche Vorfälle, die immer mehr auf dem Vormarsch sind. Machen Sie klar, dass Passwörter und ähnlich sensible Informationen nicht telefonisch oder per E-Mail herausgegeben werden dürfen.

2.63 Zombie

Ein ferngesteuerter infizierter Computer wird auch Zombie genannt. Er ist meist Teil eines Botnets.

Zombies werden häufig dazu verwendet Spam zu versenden oder Denial-of-Service-Angriffe durchzuführen und andere Systeme ebenfalls zu infizieren.

2.64 Zugangsberechtigungen

Ein zuverlässiges System für Zugangsberechtigungen ist essenziell. User sollten nur Zugang zu den Ressourcen haben, die sie tatsächlich brauchen. Außerdem muss sichergestellt werden, dass ehemalige Mitarbeiteraccounts tatsächlich ordnungsgemäß gesperrt werden. Ein Onboarding und Offboarding Checkliste, die durchgegangen wird, wenn ein neuer Mitarbeiter in das Unternehmen kommt und wenn ein Mitarbeiter das Unternehmen verlässt kann dabei helfen, keine Zugangsberechtigungen zu vergessen. Zusätzlich müssen alle Zugangsberechtigungen, die über den Standard der Checkliste hinausgehen, protokolliert werden.

2.65 Zwei Faktor Authentifizierung

Wissen Sie was 2 Faktor Authentifizierung ist? Für wichtige Dienste sollten Sie unbedingt auf die Verwendung von zwei Faktor Authentifizierung setzen. Neben einem Passwort wird für das Anmelden ein zusätzlicher Code benötigt, der in der Regel auf das Mobiltelefon via SMS oder einer Authenticator App gesendet wird. So sind Sie auch bei unbemerktem Passwort-Diebstahl geschützt, denn ohne dem Code erhalten die Angreifer keinen Zugriff. Gerade für das Administrations-Konto eines Dienstes sollte nicht auf diese Methode verzichtet werden, dann so stellen Sie sicher, dass Ihr Konto nicht so einfach von Kriminellen übernommen werden kann.

3 Sicherheits-software und -hardware

3.1 Anti-Malware

Anti-Malware-Software versucht Sie vor Viren und anderen Bedrohungen wie Würmer, Spyware und Trojanern zu schützen.

Des Weiteren enthalten Anti-Malware-Software einen Scanner, welche Programm auf mögliche Gefahren durchsucht. Dabei kann er Folgendes erkennen:

- Bekannte Malware: Er vergleicht Dateien auf Ihren PC mit bereits bekannter Malware.
- Bisher unbekannte Malware: Er analysiert Dateien auf Kennzeichen, die auf ein schädliches Verhalten hinweisen können.
- Verdächtige Dateien: Der Scanner analysiert wie sich das Programm verhalten wird und ob etwas verdächtiges sichtbar ist.

Diese Scanner sind ständig im Hintergrund aktiv und überprüfen automatisch alle neuen und bestehenden Dateien.

3.2 Appliances

Wenn Hardware und Software zu einer einzigen Sicherheitslösung kombiniert werden, spricht man von Appliances. Diese lassen sich ganz einfach anschließen ohne separate Software installieren zu müssen.

Es gibt verschiedene Typen: E-Mail-Appliances, Web-Appliances und UTM-Appliances. Sie sind dafür zuständig den Übergang zwischen IT-Systemen von Unternehmen und dem Internet sicher zu gestalten und Datenverluste zu vermeiden.

E-Mail-Appliances sind dafür zuständig vor Spam, Phishing, Spyware, Viren und anderer Schadsoftware zu schützen.

Web-Appliances stoppen ebenfalls Spyware, Malware, Phishing und andere unerwünschte Anwendungen.

UTM-Appliances vereinfachen es Einzellösungen für den Schutz von Unternehmen bereitzustellen.

3.3 Application Control

Mit Hilfe der Application Control kann festgelegt werden, welche Programme in Unternehmen laufen dürfen und welche nicht.

Damit können Sie den Zugriff für User beschränken und Richtlinien festlegen, beispielsweise welche Browser und Messenger auf einem PC installiert sein dürfen. Typische Anwendungsbereiche für Application Controls sind außerdem, P2P-Filesharing-Software, Media-Player, Spiele, Instant-Messaging-Clients und Tools zur Fernsteuerung.

3.4 Device Control

Via Device Control ist der Zugriff auf Laufwerke, Wechseldatenträger und Drahtlosnetzwerkprotokolle kontrollierbar.

Es ist ein zentrales Element, um Datenverluste zu verhindern. Zum Beispiel kann mit Hilfe einer Device Control verhindert werden, dass Malware über USB-Sticks weiterverbreitet wird. Daher setzten viele Unternehmen Device Controls ein, um bestehende Richtlinien in Bezug auf Wechseldatenträger durchzusetzen, da festgelegt werden kann, welche Medien am PC angeschlossen werden können.

3.5 Encryption/Verschlüsselung

Die Verschlüsselung von Daten ist enorm wichtig, denn nur wird das richtige Passwort weiß, kann auf die Daten zugreifen. Häufig sind Verschlüsselungslösungen so konfiguriert, dass für autorisierte Benutzer die Daten automatisch entschlüsselt werden und sie dadurch kein Passwort eingeben müssen.

3.6 Endpoint-Sicherheit

Einpoint-Sicherheitslösungen schützen Ihren Computer und andere Geräte vor verschiedenen Problemen im Bereich Sicherheit und Produktivität und können konfigurierte Unternehmensrichtlinien durchsetzen. Viele Endpoint-Sicherheitslösungen können zentral verwaltet werden.

Endpoint-Sicherheitsprodukte können folgende Features enthalten:

- Firewalls
- Device Controls
- Virenschutz
- Application Controls
- Laufzeitschutz
- Network Access Control
- Web Security
- Patch Management
- Data Loss Prevention

3.7 HTTPS-Scanning

Einige Bedrohungen können sich auch in einem verschlüsselten Datenverkehr von vertrauenswürdigen Websites verstecken. Beim sogenannten HTTPS-Scanning werden Daten entschlüsselt, gescannt und anschließend wieder verschlüsselt. So können schädliche Inhalte automatisch gefunden und entfernt werden.

3.8 IPS

IPS (Intrustion-Prevention-Systeme) überwachen Systeme und Netzwerke und stellt fest, ob schädliche Aktivitäten stattfinden. Dabei werden die Aktivitätsdaten vom System protokolliert und auf diesem Weg unerwünschte Aktivitäten blockiert.

3.9 IPsec

Mit Hilfe von IPsec kann jedes Internet-Protocol-Datenpaket (IP) einer Session authentifiziert und verschlüsselt werden und dadurch eine sichere Kommunikation ermöglicht werden.

3.10 Laufzeitschutz

Zugriffsversuche auf gefährdete Bereiche Ihres Computers können mit Hilfe eines Laufzeitschutzes blockiert werden. Er analysiert dabei das Verhalten aller ausgeführten Programme und ist in der Lage potenziell schädliche Aktivitäten zu blockieren.

Es gibt zwei verschieden Arten von Laufzeitschutzlösungen:

Host Intrusion Prevention Systeme (HIPS) scannen das Verhalten von Code und können somit Malware stoppen, bevor ein spezielles Update zur Identifizierung der Schadsoftware verfügbar ist.

Buffer Overflow Prevention Systems (BOPS) erkennen Angriffe auf Sicherheitslücken im Betriebssystem, in der Software oder in Anwendungen. Sie erfassen den Versuch, mittels Pufferüberlaufmethoden laufende Prozesse zu missbrauchen und meldet ihn sofort als Angriff.

3.11 Mobile Device Security

Auch der Schutz von mobilen Geräten ist sehr wichtig, die Mobile Device Security beschreibt dabei die Verfahren, Richtlinien und Tools zum Schutz von mobilen Geräten. Angriffe auf Smartphones haben in den letzten Jahren rasant zugenommen, und die Wichtigkeit von Mobilen Geräten ist ebenfalls so hoch wie nie zuvor. Das Schützen von mobilen Geräten mit firmeninternen Daten, sollte hohe Priorität für jedes Unternehmen haben und Mobile Geräte sollten zumindest den gleichen Schutz wie PCs erhalten.

3.12 Network Access Control (NAC)

Eine sogenannte Network Access Control (NAC) beschützt ein Netzwerk und die enthaltenen Daten vor äußeren Bedrohungen, die von angeschlossenen Geräten oder Benutzern ausgehen.

Die drei Hauptfunktionen eines NACs sind die:

- Authentifizierung von Devices und User.
- Überprüfung ob externe Geräte versuchen auf das Netzwerk zuzugreifen.
- Durchsetzung von Nutzerrichtlinien und Benutzerrollen, dass jeder User nur auf die festgelegten Daten Zugriff hat.

3.13 Spamfilter (Anti-Spam)

Unerwünschte E-Mails können mit Hilfe von Spamfiltern aussortiert werden, damit Sie nicht das Postfach des Empfängers überfluten.

Um herauszufinden, ob es sich bei einer E-Mail um Spam handelt geht ein Spamfilter wie folgt vor.

- Er blockiert E-Mails von E-Mail Adressen, die sich auf einer sogenannten „Black-List“ befinden.
- E-Mails in denen bestimmte Links enthalten sind, werden ebenfalls blockiert
- Es wird überprüft ob die Mails von einer vertrauenswürdigen Adresse stammen
- Die E-Mail wird auf bestimmte Schlüsselwörter überprüft
- Der HTML-Code der E-Mail wird auf Auffälligkeiten überprüft

3.14 Unified Threat Management

Bei sogenannten UTM-Systemen werden Sicherheitsfunktionen in einzige Netzwerk-Appliances integriert. Mit Hilfe dieser UTM-Lösungen können eine Vielzahl von Schutzschichten unkompliziert bereitgestellt und verwaltet werden.

3.15 URL-Filter und Web-Contentfilter

URL- und Webcontentfiltern ermöglichen Websites mit bestimmten Themen zu blockieren.

Da die meisten Phishing- und Malware-Angriffe über das Internet stattfinden, kann die Beschränkung von Websites verhindern, dass Mitarbeiter Opfer von Angriffen werden. Diese Filter können auch genutzt werden, um unerwünschte Websites zu blockieren.

3.16 VPN/SSL-VPN

Mit Hilfe von Virtual Private Networks (VPN) kann eine Remote-Verbindung zu einem zentralen Netzwerk hergestellt werden. Nach dem sich der Benutzer authentifiziert hat, ist es möglich mit unternehmensinternen Servern des Unternehmens zu kommunizieren. Dadurch können Sie unternehmensinterne Server nur im privaten Netzwerk verfügbar machen, wodurch sie weniger einfach angreifbar sind. Ein Angreifer muss dann erst einen Weg in Ihr Netzwerk finden, bevor er die internen Server angreifen kann.

3.17 Web Application Control

Bestimmte Anwendungen wie Instant Messaging oder P2P-File-Sharing, welche eine potenzielle Bedrohung darstellen können, werden mit Hilfe von Web Application Controls eingeschränkt.

3.18 Web Application Firewall (WAF)

Grundsätzlich ist eine Web Application Firewall wie eine herkömmliche Firewall. Sie hat jedoch noch zusätzlich Features wie Spamfilter, Inhaltsfilter, Virenschutz und Intrusion Detection. Web Application Firewalls werden üblicherweise zum Schutz von Webservern genutzt.

4 Sicherheitstipps

4.1 Wie schütze ich mich vor Viren, Trojanern, Würmern und Spyware?

Die folgenden Schutzmaßnahmen sollte Ihr Computer besitzen, um optimal geschützt zu sein.

Achten Sie darauf das Windows und andere Anwendungsprogramme stehts auf den neuesten Stand sind. Dadurch können bekannte Sicherheitslücken so schnell wie möglich geschlossen und neue Sicherheitsmechanismen so schnell wie möglich aktiv werden. Viele Programme und Betriebssysteme erlauben es, automatische Updates zu konfigurieren. Via Gruppenrichtlinien können diese häufig auch zentral verwaltet und erzwungen werden. Bei Windows Servern sollten Sie vor allem auf den zweiten Dienstag jedes Monats achten (der sogenannte „Patchday“), wo Microsoft Updates für die unterstützten Betriebssysteme gesammelt veröffentlicht.

Des Weiteren sollten Sie auf eine Firewall setzen, welche Daten überwacht, die ins Internet gesendet werden oder Sie erhalten. Anhand einer Liste können Sie verwalten, was ein Programm darf und was nicht. Sollte ein verdächtiges Programm dabei sein, schlägt die Firewall sofort Alarm. Darüber hinaus ist ein Virenschutz sehr wichtig, um die Ihren Computer vor Virenbefall zu schützen. Sobald ein Virenschutz eine verdächtige Software entdeckt blockiert Sie diese und verhindert, dass diese gestartet werden kann und im Idealfall wird der Virus auch sofort gelöscht.

Eine Erweiterung Ihres aktuellen Virenschutzes kann eine sogenannte Anti-Spionage-Software sein. Diese ist darauf spezialisiert Spionage-Programme zu erkennen.

4.2 Wie schütze ich mich vor Hoaxes?

Der beste Schutz gegen Hoaxes ist der gesunde Menschenverstand. Stellen Sie sich bei jeder E-Mail, Post oder Message die Frage, wie plausibel und glaubhaft der jeweilige Inhalt ist. Beim geringsten Hoax-Verdacht sollten Sie nicht mehr mit dieser Nachricht interagieren. Wenn Sie sich nicht sicher sind, ob es sich um einen Hoax handelt, können Sie einfach ganz einfach im Internet überprüfen, ob es sich um einen handeln könnte.

4.3 Wie schütze ich mich vor Spam?

Um sich vor Spam-Emails bestmöglich zu schützen sollten Sie folgende Dinge beachten:

- Ein gutes sicheres Passwort ist ebenso wichtig wie ein aktueller Virenschutz
- Überlegen Sie ob beispielsweise ein Link seriös ist und klicken sie nicht unüberlegt darauf
- Nutzen Sie Spam-Filter
- Geben Sie ihre E-Mail-Adresse nicht öffentlich im Netz unbedacht an
- Erstellen Sie mehrere E-Mail-Adressen für verschiedene Zwecke
- Antworten Sie niemals auf Spam-Nachrichten und klicken sie nicht auf Links
- Insbesondere bei Rechnungen oder E-Mails von angeblichen Banken sollten Sie besonders aufmerksam sein

4.4 Wie schütze ich mich vor Phishing?

Auf diese Dinge sollten Sie besonders achten, wenn Sie sich optimal vor Passwort- oder Datendiebstahl schützen möchten:

- Klicken Sie niemals auf Links einer dubiosen E-Mail und überprüfen Sie die Domain vorher
- Geben Sie auf keinen Fall persönliche Daten wie Passwörter, Transaktions- oder Kreditkartennummern über E-Mail weiter
- Geben sie Bankdaten nur auf der offiziellen Online-Banking-Website ein. Sobald Sie etwas misstrauisch sind, beenden Sie die Verbindung sofort.
- Starten Sie auf keinen Fall einen Download-Link, der sich direkt in der E-Mail befindet, da Sie sich auf dessen Echtheit nicht verlassen können. Wenn Sie etwas herunterladen möchten sollten Sie dies stehts auf der offiziellen Website tun.

4.5 Wie wähle ich ein sicheres Passwort?

Die Sicherheit eines Passworts steigt in erster Linie mit der Länge. Beispielsweise ist das Passwort "lgwervawfewdaj" deutlich sicherer und schwerer zu erraten als "g!G424" Es ist nicht realistisch sich für jeden Dienst ein eigenes, langes und zufälliges Passwort zu merken, daher empfehlen wir, einen Passwortmanager zu verwenden. Vom ständigem Passwort-Wechseln raten wir ab, Studien zeigen, dass damit nur die Qualität der selbst gewählten Passwörter sinkt. Wir empfehlen jedoch, sich für möglichst viele Accounts ein sicheres Passwort von dem Passwortmanager generieren zu lassen.

4.6 Wie sichere ich meine Daten?

Auf jedem Computer kann es aus verschiedensten Gründen wie z.B. Hardware-Defekten, Software-Fehlern oder durch Virenbefall, zu einen Datenverlust kommen. Daher sollten Sie sich dahingehend gut absichern, da ansonsten eine große Menge an Zeit und Geld verloren gehen kann.

Es gibt verschiedene Möglichkeiten, um seine Daten zu sichern. Die drei wichtigsten Methoden sind die folgenden:

- **Datensicherung auf externen Festplatten**
  Regelmäßige Sicherung der Daten auf einer externen Festplatte.
- **Online Backup**
  Alle Daten werden hierbei regelmäßig mit einem Online Backup-Service synchronisiert.
- **Sicherung auf einem Netzwerkspeicher**

Regelmäßige Sicherung der Daten im eigenen Netzwerk/Zuhause auf einem Netzwerkspeicher (NAS)

4.7 Wie verwende ich Wechseldatenträger sicher?

Die Benutzer einschulen

Nicht alle Benutzer sind sich der Gefahren bewusst, die von Wechseldatenträger, USB-Sticks oder CDs ausgehen. Die Verbreitung von Malware und mögliche Datenverluste wären ein Beispiel dafür. Daher wäre eine Schulung wichtig, um auf diese Gefahren aufmerksam zu machen.

Gerätetyp Identifizieren

Legen Sie für die oben genannten Geräte bestimmte Beschränkungen und Genehmigungen fest.

Device Control implementieren

Überprüfen Sie, welche Datenträgertypen erlaubt sind und welche Daten ausgetauscht werden dürfen. Dadurch kann die Sicherheit im Netzwerk erhöht werden. Entscheiden Sie sich daher für ein Produkt, welches Beschränkungen und Genehmigungen Gerätegruppen oder einzelne Geräte festlegen kann.

Verschlüsseln Ihrer Daten

Die Verschlüsselung von Daten schützt vor Datenverlust. Speziell bei Wechseldatenträger, welche man leicht verlieren kann oder gestohlen werden können. Dank moderner Verschlüsselungstechnologien können unberechtigte Dritte Personen die Daten weder kopieren noch lesen.

4.8 Wie tätige ich sichere Online-Käufe

Leider ist es häufig nicht mit dem bloßen Auge zu erkennen, ob eine Website seriös und sicher ist oder nicht. Häufig werden Websites, die keinen ausreichenden Schutz haben, von Hackern angegriffen. Der Kunde der online einkaufen möchte bemerkt davon häufig nichts und wird unwissend angegriffen.

Doch was kann ich tun, um mich vor solchen Gefahren zu schützen?

- **Achten Sie auf Prüfsiegel oder Zertifikate**
  Einer der sichersten Indizien für eine seriöse Website ist ein Prüfsiegel oder ein Zertifikat einer anerkannten Prüfstelle.
- **Bewertungen**
  Neben Gütesiegeln und Zertifikaten sind Online-Erfahrungsberichte und Kundenbewertungen eine gute Möglichkeit, einen seriösen Online-Shop zu erkennen. Recherchieren Sie über die Suchmaschine nach diesen Gütesiegeln, den die Grafiken auf der Website könnten gefälscht sein.
- **Falsche Bewertungen**
  Man darf jedoch nicht jede Bewertung für einen sicheren Indiz für einen seriösen Shop halten. Viele Online-Shops enthalten jedoch gefälschte Kundenrezessionen, was zu einem ernstzunehmenden Problem wurde. Es gibt jedoch einige Möglichkeiten, wie sie falsche Bewertungen erkennen können. Ein Beispiel dafür wären viele übertrieben positive Bewertungen innerhalb kurzer Zeit, identische Nutzername die sehr viele Produkte auf dieser Seite gekauft haben oder Bewertungen, die vielmehr an eine Werbung erinnern als an konstruktives Feedback.
- **Sichere Passwörter**
  Um Ihre Passwörter so sicher wie möglich zu gestalten empfehlen wir ein Passwort länge von mindestens acht Zeichen, die eine Mischung aus Buchstaben, Zahlen und Sonderzeichen enthält. Sie sollten für jeden Account ein vollständig anderes Passwort nutzen (nur einige Zeichen variieren ist nicht genug!). Um sich diese vielen verschiedenen Passwörter merken zu können empfehlen wir einen Passwortmanager.
- **Sicheres Bezahlen**
  Wenn Sie online bestellen stehen Ihnen meist unterschiedliche Bezahlmethoden zu Auswahl. Als sichere Zahlungsmethoden gelten beispielsweise:
  - Bezahlung per Rechnung,
  - Bezahlung per Nachnahme,
  - Zahlung per Kreditkarte,
  - Zahlung per Lastschrift,
  - Zahlung per PayPal

5 Quellen

- Sophos
- Schindler-IT Solutions