CYBERSECURITY
EXPERTS ON YOUR SIDE

RATGEBER
HOME-OFFICE

ESET.DE | ESET.AT | ESET.CH

INHALTSVERZEICHNIS

CORONA-EFFEKT: 68 PROZENT DER BESCHÄFTIGTEN WOLLEN NACH DER KRISE NICHT DAUERHAFT ZURÜCK

41 Prozent der Beschäftigten arbeiten derzeit von zu Hause. Das ist ein Ergebnis der repräsentativen ESET-Studie „Veränderung der Arbeitswelt durch Corona", die im Auftrag des europäischen IT-Sicherheitsherstellers von YouGov im April 2020 durchgeführt wurde. Doch wie sieht es nach der Corona-Krise aus?

68 Prozent der Beschäftigten wünschen sich eine Lockerung der Regelungen. Sie wollen entweder mindestens einen Tag in der Woche von zu Hause arbeiten (29 Prozent), flexibel entscheiden können, ob sie im Heimbüro oder in der Dienststelle tätig sind (31 Prozent). Acht Prozent der Mitarbeiter können sich sogar ein Arbeitsleben ohne festen Arbeitsplatz im Firmengebäude vorstellen.

Die Ergebnisse zeigen: Das Thema Digitalisierung ist auch nach Ende der Ausnahmesituation dringlicher denn je. Unternehmen kommen auf Dauer nicht umhin, ihren Mitarbeitern ein verändertes Arbeitsumfeld zu bieten. Das bedeutet, dass das Thema IT-Sicherheit schnellstmöglich wieder auf die Unternehmensagenda zu setzen, damit Heimarbeitsplätze nicht zu „trojanischen Pferden" für den Schutz von Firmendaten werden. Auch hier zeigt die Studie einen großen Nachholbedarf nach der Krise.

„Die Corona-Krise hat die Digitalisierung in den Unternehmen beschleunigt und auch vielen Mitarbeitern ungewohnte Freiheiten in ihrer Arbeitswelt eingeräumt. Beim Thema IT-Sicherheit sehen wir bei Firmen noch einen gravierenden Nachholbedarf", erklärt Holger Suhl, Country Manager DACH bei ESET. „Nicht einmal jeder Dritte hat für die Arbeit in den heimischen vier Wänden eine volle technische Ausstattung und IT-Richtlinien von seinem Arbeitgeber erhalten, 14 Prozent nutzen für berufliche Zwecke ihre privaten Geräte – nicht nur aus Sicht der Datensicherheit ein GAU."

Anzahl der Heimarbeit ist rasant gestiegen

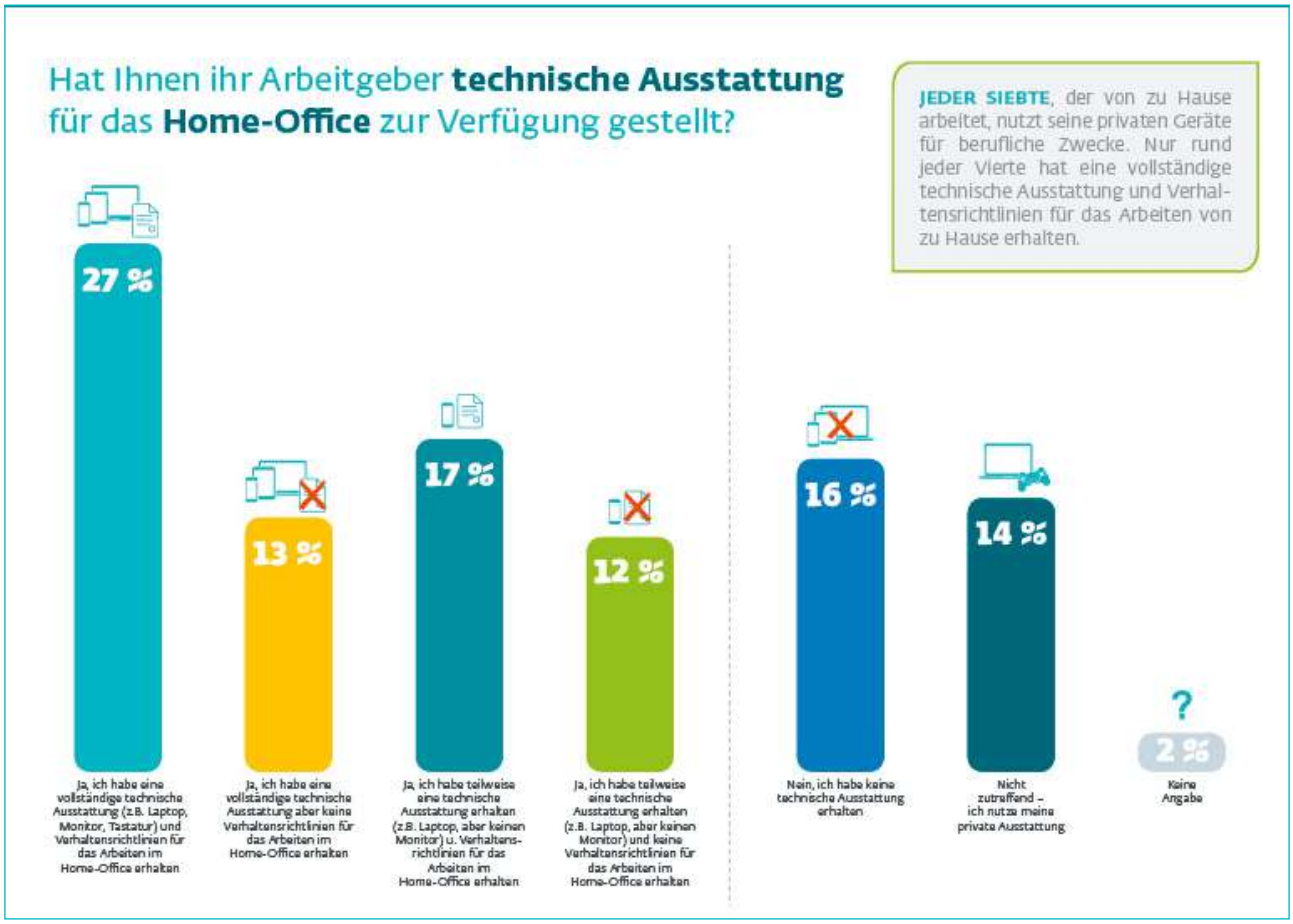
Fast die Hälfte der Beschäftigten (41 Prozent) sind derzeit von zu Hause tätig. Davon wurden fast 70 Prozent erst durch die aktuelle Situation ins Home-Office geschickt. „Es mussten von einem Tag auf den anderen Infrastrukturen geschaffen werden, die es Mitarbeitern erlauben, in den eigenen vier Wänden zu arbeiten. Improvisieren stand auf der Tagesordnung. Das gilt es, für die Zukunft auf stabile Füße zu stellen", so Suhl.

Rüstzeug für das Arbeiten von zu Hause häufig nur unzureichend

Nur 27 Prozent der Befragten wurden von ihrem Arbeitgeber mit kompletter Technik und Verhaltensrichtlinien für die Arbeit im Home-Office ausgestattet. Ein Viertel hat keinen IT-Leitfaden bekommen, was es im Heimbüro zu beachten gilt. „Die Ergebnisse sind erschreckend. Gerade der Einsatz einer VPN-Software sowie einer Multi-Faktor-Authentifizierung ist essenziell, um die Zuverlässigkeit des Unternehmensnetzwerks sicherzustellen. Benutzername und Passwort reichen in dieser Situation bei weitem nicht mehr aus“, erklärt Holger Suhl. Überraschend: Rund 30 Prozent der Befragten haben gar keine technische Ausstattung erhalten (16 Prozent) oder nutzen ihre privaten Geräte für berufliche Zwecke (14 Prozent). „Mit Blick auf die Datensicherheit und die Sicherheit des Unternehmensnetzwerks ist das grob fahrlässig. Im Schadensfall ist es zweifelhaft, ob zum Beispiel eine Cyberversicherung hier einspringt.“

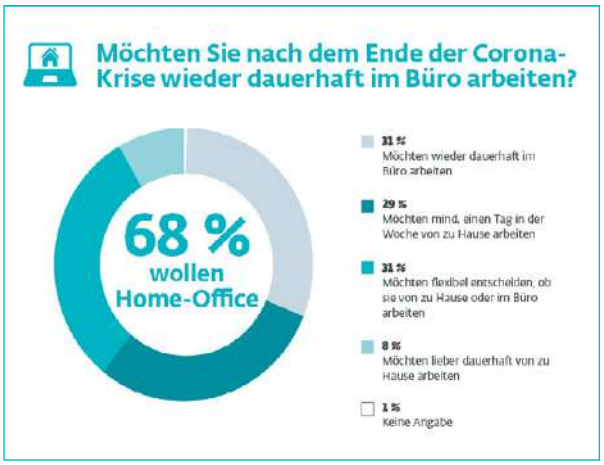
Und nach den Beschränkungen? Beschäftigte sind gespalten

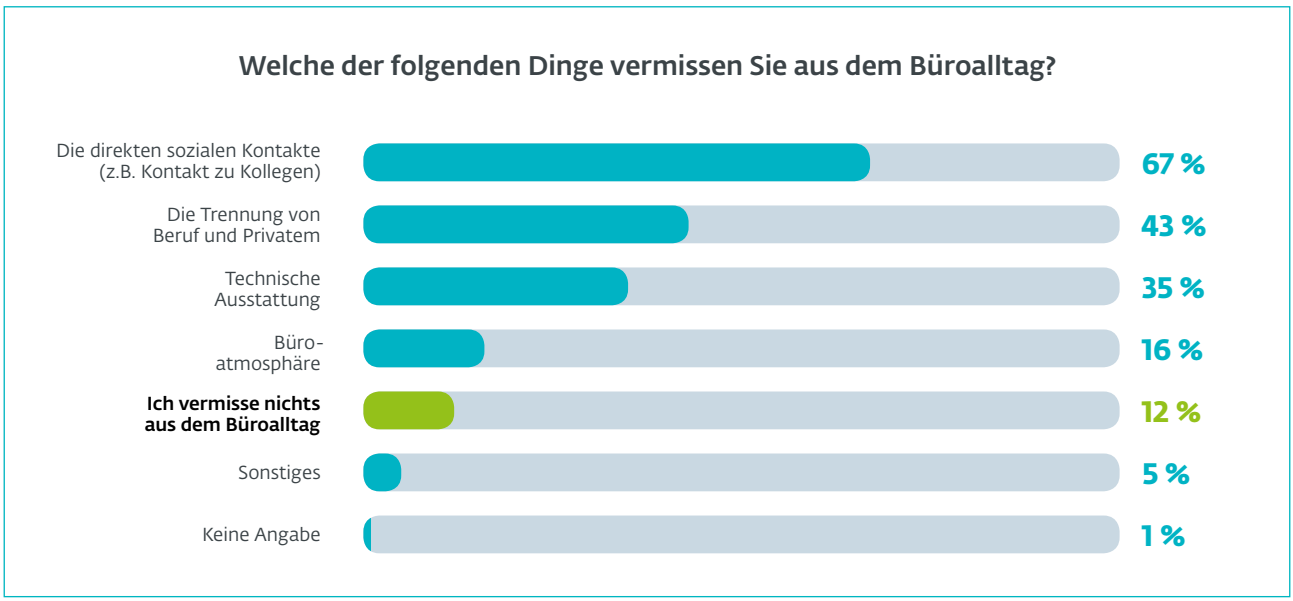
Fast jeder Dritte möchte nach dem Ende der Corona-Krise wieder dauerhaft zurück ins Büro. Ganze acht Prozent wollen gar nicht mehr zurück ins Büro. 60 Prozent der Beschäftigten wünschen sich eine Lockerung der Regelungen. Sie wollen entweder mindestens einen Tag in der Woche im Home-Office tätig sein (29 Prozent) oder flexibel entscheiden können, ob sie von zu Hause oder im Büro arbeiten (31 Prozent). „Unternehmen, die vor Corona strikt gegen Home-Office waren, werden zukünftig umdenken und ihren Mitarbeitern flexible Arbeitsmodelle einräumen müssen. Nach gut einem Monat im Home-Office ist es an der Zeit, die Absicherung der Arbeitsplätze in den eigenen vier Wänden in den Fokus zu rücken. Hierbei ist ein sicherer Zugriff auf das Firmennetzwerk durch Multi-Faktor-Authentifizierung elementar“, so Suhl.

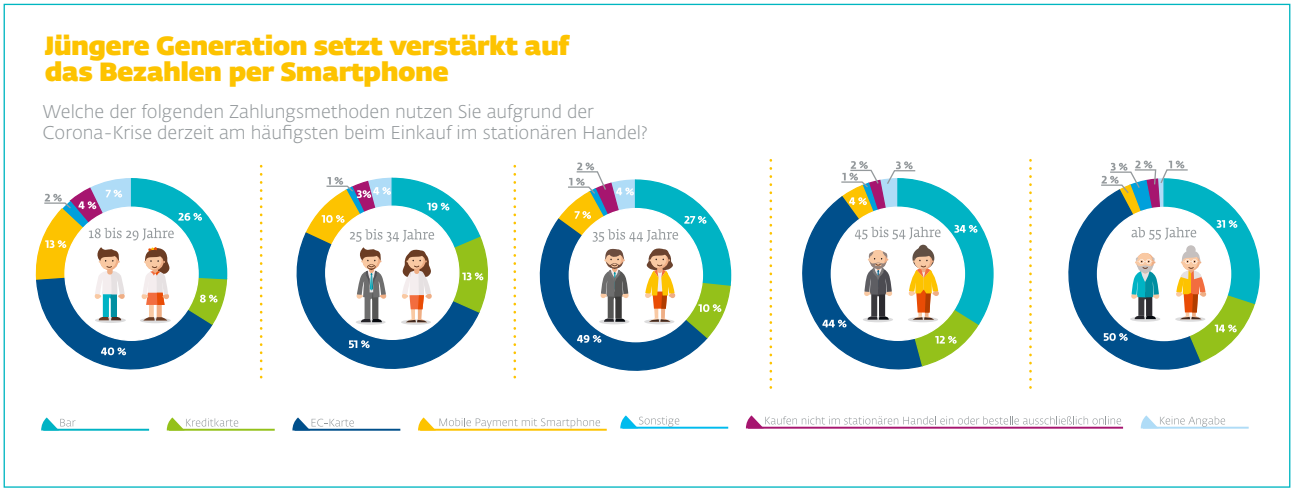


Über die Umfrage

Für die ESET-Studie „Veränderung der Arbeitswelt durch Corona“ wurde eine Online-Umfrage von YouGov Deutschland GmbH durchgeführt, an der 2045 Personen im Zeitraum vom 07.04.2020 bis 09.04.2020 teilnahmen. Die Ergebnisse wurden gewichtet und sind repräsentativ für die deutsche Bevölkerung ab 18 Jahren.







HOME-OFFICE – ORGANISATORISCHE SECURITY-TIPPS FÜR UNTERNEHMEN

Als Vorsichtsmaßnahme gegen die Verbreitung des Coronavirus verlagern sich aktuell viele Arbeitsplätze in die heimischen vier Wände. Nicht alle Arbeitnehmer und -geber sind darauf vorbereitet. Wie ist also zu tun, um möglichst sicher von zu Hause aus weiterarbeiten zu lassen?

Die aktuelle Situation verdeutlicht, wie wichtig vorausschauende Planungen sind. Doch so manches Konzept wird zu schnell von der Realität überrollt oder einfach zu lange auf die lange Bank geschoben. So finden sich derzeit viele Arbeitgeber mit der Situation konfrontiert, „business as usual" so gut wie möglich vom Heimarbeitsplatz zu betreiben. Weil es an der Ausstattung mit firmeneigener Hardware wie Laptops vor allem in kleineren Unternehmen mangelt, nutzen auch viele Angestellte Ihr privates Notebook oder Tablet. Damit sollen sie möglichst sicher Unternehmensdaten bearbeiten oder auf die Server der Firma zugreifen. Aber wie?

Keine Panik, Überblick verschaffen

- Welche Mitarbeiter/Abteilungen des Unternehmens können ihre Tätigkeiten von zu Hause erledigen?
- Verfügen diese bereits über die entsprechende IT-Ausstattung?
- Falls nein, gibt es die Bereitschaft der Mitarbeiter, die Arbeit von zu Hause mit privaten Geräten zu erledigen?
- Wie sieht unsere IT Infrastruktur aus? Welche Server in welchen Rollen, welche Clouddienste, welche Software in welchem Lizenzumfang nutzen wir?
- Erlaubt es die Bandbreite am Firmenstandort, dass auf das Netzwerk zugreifen können?
- Wie ist unser IT Team aufgestellt? Haben/brauchen wir externe Hilfe?

Saubere, einfache Dokumentation

Stellen Sie sicher, dass die Mitarbeiter mit allen notwendigen Informationen ausgestattet sind. Sie können in Form von Dokumenten (digital oder ausgedruckt), über das Intranet oder Webseiten bereitgestellt werden. Letztere Varianten haben den Vorteil, dass sie immer um aktuellste Informationen ergänzt werden können. Es ist entscheidend, dass die Mitarbeiter die (teilweise neuen) Technologien, die in den nachfolgenden Punkten beschrieben werden, sicher bedienen können.

Dokumentieren Sie außerdem alle internen Schritte, um sie jederzeit überprüfen und anpassen zu können und den Überblick zu behalten.

Clouddienste überprüfen

Bei diesem Thema denken viele schnell an Microsoft Office 365, an Dropbox und Co. Mancher auch an Microsoft Azure oder Amazon Web Services. Aber zu den Clouddiensten gehören noch andere Services, wie der Mailserver eines Drittanbieters oder des Webseitenbetreibers. Dazu zählt auch die gehostete Webseite. Kurzum: Alles, was sich weder auf Ihren eigenen Servern und Computern oder denen Ihrer Mitarbeiter befindet. Nicht allen Unternehmen ist klar, welche dieser Dienste in welchem Umfang genutzt oder in der neuen Situation hinzugebucht werden sollten.

Fragen, die es jetzt zu beantworten gilt:

- Ist es überhaupt möglich, dass alle Mitarbeiter remote auf alle benötigten Dienste zugreifen können?
- Wer ist für die Datensicherheit der Cloudangebote verantwortlich, falls doch etwas passiert?
- Wer ist für die regelmäßige Aktualisierung zuständig? Das bezieht sich auf Betriebssysteme Management Systeme von Webangeboten uvm.
- Gibt es die Möglichkeit, zusätzliche Security Optionen zu buchen?
- Welche Rechtsprechung gilt / wo stehen die Server des Angebots?

Hier gilt es also, bestehende und abzuschließende Verträge und EULA genauestens zu prüfen und anzupassen.

Digitale Meetings

Eine der Herausforderungen in der täglichen Arbeit, ist die Umsetzung von regelmäßigen Meetings bei (physischem) Kontaktverbot. Eine nahezu unendliche Auswahl an Tools und Plattformen bietet sich hier an.

Die klassische Telefonkonferenz ist eine Variante, die sich schnell umsetzen lässt. Je nach Größe des Teams kann man das mit modernen Smartphones selbst abbilden, ohne dass eine teure Telefonanlage benötigt wird. Soll auch visuell kommuniziert werden, sind Videoplattformen erforderlich. Für Unternehmenslösungen müssen an dieser Stelle entsprechend ausreichend Lizenzen und Bandbreite verfügbar sein. Sollen die Mitarbeiter über ihre privaten Geräte teilnehmen, können Sie schlecht eine Lösung vorschreiben, weswegen auf vorhandene Apps zurückgegriffen wird.

Achten Sie jedoch darauf, wer diese anbietet und wie es um die Datenschutzbestimmungen der Softwares bestellt ist. Von der Verwendung der Videotelefonie-Funktion von WhatsApp und dem Facebook Messenger wird bei unternehmenskritischen Gesprächen abgeraten, da der Facebook-Konzern sich vorbehält, einzelne Gespräche auszuwerten. Sie möchten sicherlich vermeiden, dass Firmeninterna mit Facebook geteilt werden. Ähnliches gilt für die Privatanwenderversion von Skype. Bei geschäftskritischen Gesprächen sollten Sie auf verschlüsselte Telefonate per Threema, Signal, Telegram & Co. zurückgreifen – wobei Sie auf Bildübertragungen verzichten müssen.

Und auch wenn teaminterne WhatsApp Gruppen bequem sind, sollten keine Firmendateien über diese Gruppen versendet werden. Dateien sollten lieber als verschlüsselte Mail oder wo das nicht möglich ist, per verschlüsselter Übertragung durch ein VPN am Firmenserver ausgetauscht werden.
Sollten Sie mit der Situation und den Hand-lungsempfehlungen an Grenzen stoßen, egal ob personell oder des Verständnisses, stehen Ihnen spezialisierte Dienstleister, wie Managed Services Provider, gerne zur Verfügung. Anderweitige Informationen bezüglich der Mitarbeiter, bei denen Heimarbeit nicht möglich ist, sowie aktuelle Informationen zu möglichen Soforthilfen finden Sie auf den Webseiten der IHK, des BVMW und Ihrer jeweiligen Landesregierungen.

HOME-OFFICE – SICHERER ZUGRIFF AUF DAS FIRMENNETZWERK

In der Corona-Krise arbeiten derzeit viele Mitarbeiter den eigenen vier Wänden. Gera-de Arbeitgeber stehen vor enormen Herausforderungen. Sie kommen in der jetzigen Situation nicht umhin, in neuen Bahnen zu denken und zu agieren – insbesondere bei der IT-Sicherheit.

Gerade kleine Unternehmen sind mit der aktuellen Situation überfordert und suchen händeringend nach wirksamen Hilfestellungen und Lösungen. Die Anforderung ist klar: Mitarbeiter sollen so normal wie möglich vom Heimarbeitsplatz weiter tätig sein. An vielen Stellen fehlen allerdings Vorkehrungen für eine solche Notsituation. Nicht alle Unternehmen haben die Möglichkeit, ihre Angestellten mit firmeneigener Hardware wie Laptops auszustatten. Nicht wenige Mitarbeiter sitzen nun vorm privaten Laptop, PC oder Tablet und sollen möglichst sicher Unternehmensdaten bearbeiten oder auf die Server der Firma zugreifen.

Wie kann also der Zugriff auf die Unternehmensnetzwerke sichergestellt werden? Welche ist die richtige VPN-Lösung, um die Kommunikation zu schützen? Warum sollten Mitarbeiter eine Multifaktor-Authentifizierung verwenden, um sich an den Unternehmensdiensten anzumelden?

VPN Lösungen

VPN („Virtual Private Network“) Lösungen erstellen einen verschlüsselten „Kommunikationstunnel“ zwischen einem Endgerät, das egal wo in der Welt steht, und Ihrem Netzwerk. Nur so sorgen sie dafür, dass niemand die Kommunikation mitschneiden oder anderweitig manipulieren kann. Nicht jedes WLAN, in dem sich die Geräte der Nutzer befinden, ist gleich sicher. Ihr Unternehmen benötigt also eine VPN Serverlösung mit der Möglichkeit, auf den Geräten der Mitarbeiter eine entsprechende Clientsoftware zu installieren. Falls dies auf privaten Geräten geschieht, denken Sie bitte an eine lückenlose Anleitung.

Bei der Auswahl der VPN Lösung sollten Sie zudem darauf achten, dass sie entsprechend der Mitarbeiterzahl ausreichend lizensiert ist. Haben Sie bereits eine Lösung im Einsatz, überprüfen Sie ebenfalls, ob die ursprüngliche Lizenzgröße noch ausreicht.

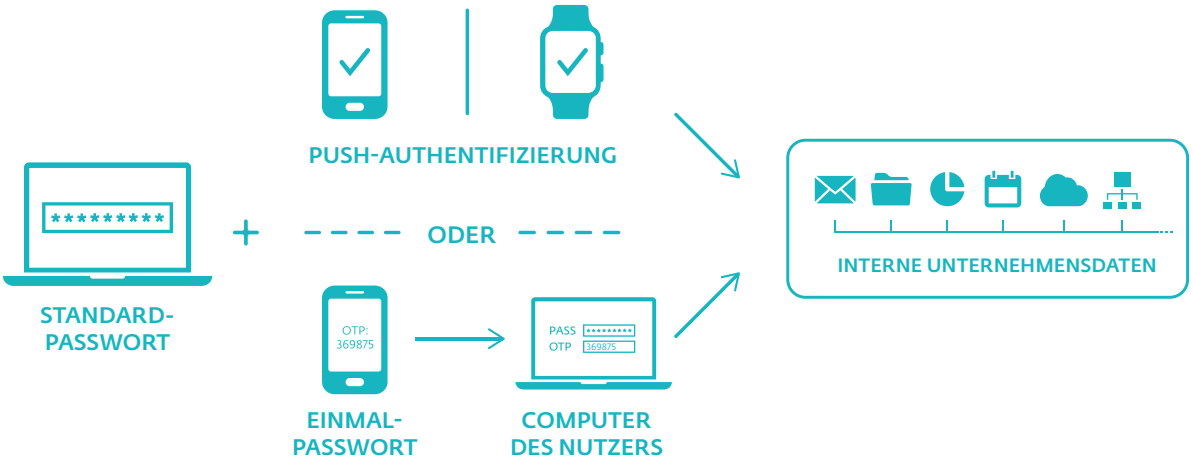
2- oder Multifaktor Authentifizierungen

Die klassische Anmeldung per Benutzername und Passwort birgt nachweislich viele Risiken: Verlorene, erratene, gestohlene, zu einfache und wiederverwendete Passwörter höhlen jedes noch so gute Sicherheitskonzept aus. Abhilfe schaffen hier 2-Faktor-Authentifizierungen (2FA), auch als „Anmeldung in zwei Schritten" oder Multifaktor-Authentifizierung (MFA) bezeichnet. Das zugrunde liegende Prinzip ist, dass zusätzlich zum Benutzernamen und Passwort ein Einmal-Code für die Anmeldung an den Unternehmensdiensten notwendig ist. Dieser kann per SMS verschickt, in einer entsprechenden App auf dem Smartphone des Nutzers oder als Push-Nachricht mit Ja-Nein-Abfrage auf dem selbigen realisiert werden. Außerdem lassen sich noch Authentifizierungsgeräte, die per USB am Rechner angeschlossen werden, verwenden.

Desktop Protokoll (RDP) überall deaktiviert werden, wo es nicht dringend benötigt wird, da Cyberkriminelle immer wieder über diese, in Windows standradmäßig aktive „Hintertür" in Unternehmensnetze eindringen. Dort, wo RDP nicht deaktiviert werden kann, sollte 2FA aktiv sein, um folgende Anmeldungen an Windowssystemen entsprechend abzusichern.

Verschlüsselung

Beim Übertragen von Unternehmensdaten über das Internet ist natürlich höchste Vorsicht geboten. Kriminelle versuchen, die aktuelle Notsituation durch Spam und andere Angriffe für sich auszunutzen. Deswegen ist eine konsequente Verschlüsselung in allen Bereichen unabdingbar! Die Verschlüsselung beginnt bei der Übertragung: Ihre Webdienste sollten generell nur per HTTPs aufrufbar sein, VPN-Lösungen soll-



Unternehmen, die solche Lösungen beispielsweise aus Budgetgründen noch nicht im Einsatz haben, bietet ESET aktuell als Soforthilfemaßnahme die eigene Lösung ESET Secure Authentication für sechs Monate, ohne automatische Verlängerung kostenfrei zur Verfügung. Eingerichtet ist ESA in circa zehn bis 15 Minuten und das Produkt lässt sich „Stand Alone" betreiben. Andere ESET Software ist also keine Voraussetzung.

Im Zuge des Anmeldungsprozesses sollten Sie außerdem die Zugriffsrechte auf einzelne Speicherorte und Dienste überprüfen. Weiterhin sollte das Remote

ten den Kommunikationskanal verschlüsseln. Gute Unternehmenslösungen zur Verschlüsselung bieten zudem noch viele weitere notwendige Optionen. So sollten alle Dateien, die über Drittanbieterdienste (wie WeTransfer oder Cloudspeicher von Google, Microsoft & Co.) oder per E-Mail ausgetauscht werden, verschlüsselt werden und vieles mehr.
Ist eine solche Lösung noch nicht vorhanden, ist es in der Übergangsphase umso wichtiger, dass zur Anmeldung bei den Cloudspeichern eine 2FA zum Einsatz kommt. Diese gibt es in Form des Google Authenticators oder auch von Microsoft kostenfrei und es lassen sich mehrere Dienste in einer App zusammenfassen.

Mittel- und langfristig kann aber eine solche Lösung nicht die Verschlüsselung ersetzen!

Weitere Informationen

Anderweitige Informationen bezüglich der Mitarbeiter, bei denen Heimarbeit nicht möglich ist, sowie aktuelle Informationen zu möglichen Soforthilfen finden Sie auf den Webseiten der IHK, des BVMW und Ihrer jeweiligen Landesregierungen.

Sollten Sie mit der Situation und den untenstehenden Handlungsempfehlungen an Grenzen stoßen, egal ob personell oder des Verständnisses, wenden Sie sich am besten an spezialisierte, kompetente Dienstleister wie Managed Services Provider.

Weiterführende Informationen:

- https://www.eset.de/sicheres-home-office
- https://www.eset.de/business/secure-authentication/
- https://www.welivesecurity.de
- https://www.eset.com/de/about/presse/presse-mitteilungen/pressemitteilungen/eset-startet-hilfsaktion-fuer-unternehmen-zur-absicherung-von-home-offices/

HOME-OFFICE – VIRENSCHUTZ, BACKUP UND DANN?

Kriminelle schlafen nie. Im Zusammenhang mit der Corona-Pandemie sehen wir aktuell eine Vielzahl an Spam- und Phishing-Mails. Kriminelle Trittbrettfahrer nutzen die Verunsicherung der Bevölkerung schamlos aus und wollen vom analogen Virus profitieren.

Angebliche News zu Covid-19 von renommierten Instituten wie der Weltgesundheitsorganisation (WHO) oder populären Nachrichtenportalen, vermeintliche Spendenaufrufe oder sagenhafte Angebote von Atemschutzmasken, die Nutzer auf Fake-Shops leiten – Cyberkriminelle nutzen im Moment alles aus, was ihren illegalen Tätigkeiten zum Erfolg verhilft.

Neben diesen Aufhängern bei Cybercrime-Kampagnen laufen zum Beispiel Ransomware-Attacken auf Unternehmen in unverminderter Intensität weiter. Die Verschlüsselungstrojaner sind eine große Gefahr für Unternehmensnetzwerke. Gerät so ein Schadprogramm im Umlauf, kann das für einen Betrieb teure Produktionsausfälle und Datenverluste bedeuten.

Eine ganzheitliche Sicherheitslösung und eine Backup-Strategie sind für den Schutz des Firmennetzwerks unerlässlich, egal ob die Mitarbeiter im Büro oder aus dem Home Office arbeiten. Doch was ist in der aktuellen Situation zu beachten? Wie realisieren Administratoren nun regelmäßige Sicherungskopien?

Wie muss die Sicherheitsstrategie in Bezug auf die eingesetzte Antimalware-Lösung angepasst werden? Wie geht eine IT-Abteilung schlimmstenfalls in diesem Kontext mit einer Vielzahl von Fremdgeräten im Netzwerk um? Auf diese und weitere Fragen werde ich Ihnen im folgenden Lösungsszenarien aufzeigen.

Gerne gehe ich auf einen Punkt ein, der wahrscheinlich erst nach diesen Maßnahmen greifen wird, aber enorm wichtig ist: Monitoring. Sind die Herausforderungen gemeistert, die ich in dieser Artikel-Serie aufgezeigt habe, gilt es, den Sicherheitsstatus des Unternehmensnetzwerks im Blick zu behalten.

Hier nun meine Tipps für die Wahl der richtigen Antimalware-Lösung, einer intelligenten Backup-Strategie sowie der Überwachung des Sicherheitsstatus.

Backups

Sicherungskopien sind immer wichtig. Auch wenn sie im Angesicht der aktuellen Lage sogar noch mehr an Bedeutung gewinnen, werden sie oft vergessen. Entgegen der Versprechen einiger Cybergangster laufen Ransomware-Attacken auf Unternehmen unvermindert weiter. Manche Kriminelle räumen zwar einen „Corona-Rabatt" bei den Lösegeldforderungen ein, aber der Schaden bleibt dennoch enorm – alleine schon durch die entstandenen Produktivitätseinbußen.

Ob Firmen ihre Daten jemals wiedersehen, ist eine andere berechtigte Frage: Wenn sie das Lösegeld zahlen, dann in den meisten Fällen erfolglos. Umso wichtiger bleiben regelmäßige, intelligente Backups, sodass saubere Sicherungen der kriminellverschlüsselten Daten schnellstmöglich eingespielt werden können, ohne große Ausfallzeiten oder Lösegeldzahlungen in Kauf nehmen zu müssen.

Eine andere Notwendigkeit ergibt sich aus der „fragmentierten" Datenübertragung. Zugriffe auf Kollaborativserver aus verschiedenen Netzwerken über verschiedene Übertragungswege führen durchaus zu Verbindungsabbrüchen. Kollegen, die ausversehen das Masterdokument vom Server löschen und Hardware, die aufgrund der gesteigerten Anforderungen plötzlich ausfällt: Hier sind Backups bares Geld wert! Planen Sie also intelligente Sicherungsvorgänge und prüfen Sie regelmäßig auch ob die Wiederherstellung aus Backups funktioniert.

Wichtig: Trennen Sie nach dem Sicherungsvorgang die USB- und Netzwerkspeichermedien vom System. Ransomware verschlüsselt in den meisten Fällen alle vom System aus erreichbaren Speichermedien mit.

Zusätzliche Schutzsoftware

Home-Office vergrößert die Zugangswege für Cyberkriminelle um ein Vielfaches. Deswegen ist es entscheidend, mögliche Angriffsvektoren zu kennen und abzusichern. Malware, Spam, Phishing, Fake-Webseiten wollen sicher und datenverlustarm bekämpft werden. Der Windows Defender ist an dieser Stelle keine wirkliche Hilfe, da er über einen begrenzten Funktionsumfang verfügt. So ist er nicht in der Lage, Webseiten und Emails zu überprüfen – beides Haupteinfallstore für Schadsoftware.

Wird ein anderer Browser als Microsoft Edge verwendet und wurden aus Compliance- oder Datenschutzgründen die SmartScreen Filter von Windows deaktiviert, prüft der Windows Defender nur noch das lokale Gerät auf Dateiebene. Malware, die Scripte über infizierte Webseiten startet, die in den RAM des Rechners geladen, dort entpackt, entschlüsselt und ausgeführt werden, kann er nicht erkennen und blockieren.

Deswegen braucht es jetzt Unternehmenslösungen zum Schutz vor Malware! Sie müssen auf den Gateway-, File- und Mailservern installiert werden sowie

natürlich auf den Endgeräten der Nutzer. Dabei sollten alle Installationen von einer Konsole aus verwaltet werden können. Das gilt allerdings nur, wenn Mitarbeiter auf firmeneigener Hardware arbeiten. Müssen Anwender ihre Privatrechner fürs Home-Office nutzen, ist die Situation weitaus schwieriger. Unternehmen dürfen in dem Falle keine installierte Software vorschreiben. Sie haben aber folgende Möglichkeiten:

- Bitten Sie die Mitarbeiter (schriftlich!) um Erlaubnis, die Clientsoftware Ihres Antimalware-Herstellers auf den privaten Geräten installieren zu dürfen. Entscheidend ist dabei, dass Sie auch darüber informieren, wie mit den Daten der Nutzer umgegangen wird. Erklärun gen dazu finden Sie beim Hersteller. Außerdem ist es wichtig, darüber zu informieren, was mit und auf den Geräten passiert, sollte es zu einer Virenwarnung kommen.

- Fragen Sie beim Hersteller Ihrer Antimalware-Lösung nach, ob und in welcher Form er Mitarbeiterlizenzen anbietet, womit die Nutzer die Heimanwendersoftware des Herstellers selbst installieren und verwalten können.

- Achtung! Das Finanzamt sieht hier unter Umständen einen geldwerten Vorteil und verlangt eventuell zusätzliche Steuerabgaben!

- Alternativ können Sie die Mitarbeiter bitten, eine Antimalware-Lösung des Vertrauens zu installieren. Klären Sie darüber auf, dass weder der Windows Defender noch andere, kostenfreie Tools vollumfassend schützen. Manche Anbieter verzichten auf wichtige Schutzfunktionen, andere verkaufen zudem die Nutzerdaten (und unter Umständen die Firmendaten) für Werbezwecke.

- Bitten Sie bei installierten eigenen Softwares die Nutzer darum, vor Beginn der Heimarbeit einen Tiefenscan des Systems mit schärfsten Einstellungen durchzuführen, um „schlummernde" Gefahren aufzuspüren. Sollte etwas gefunden werden, sollten sich Mitarbeiter an den IT-Support wenden, bevor sie die Arbeit aufnehmen.

So oder so gilt: Alle Software und auch die Betriebssysteme sollten immer mit den neuesten Updates versorgt werden. Nur so lassen sich Sicherheitslücken schnellstmöglich schließen und neue Angriffswellen effektiv bekämpfen!

Ständiges Monitoring

Dieses Thema betrifft vorrangig Ihr IT-Team und/oder Ihren IT-Dienstleister. Gerade in der aktuellen Situation sollten Sie einen ständigen Überblick über die unten aufgeführten Punkte haben. Da dies recht viel werden kann, setzen Sie auf Lösungen, wie etwa beim Thema IT-Security, die Ihnen für viele Zwecke einen hohen Automatisierungsgrad bieten. Folgendes sollte also überwacht werden:

- Achten Sie auf die Verbindungen zu und von Ihrem Netzwerk nach den Endpunkten, Protokollen und wo es möglich ist, der Anwendung, die die Verbindung aufgebaut hat.

- Haben Sie fehlgeschlagene Login-Versuche im Blick. Ein oder zwei Fehlversuche können durch Falscheingaben oder Verbindungsabbrüche schnell zustande kommen. 15 Fehlversuche oder mehr in 15 Minuten deuten dagegen auf einen Angriffsversuch hin.

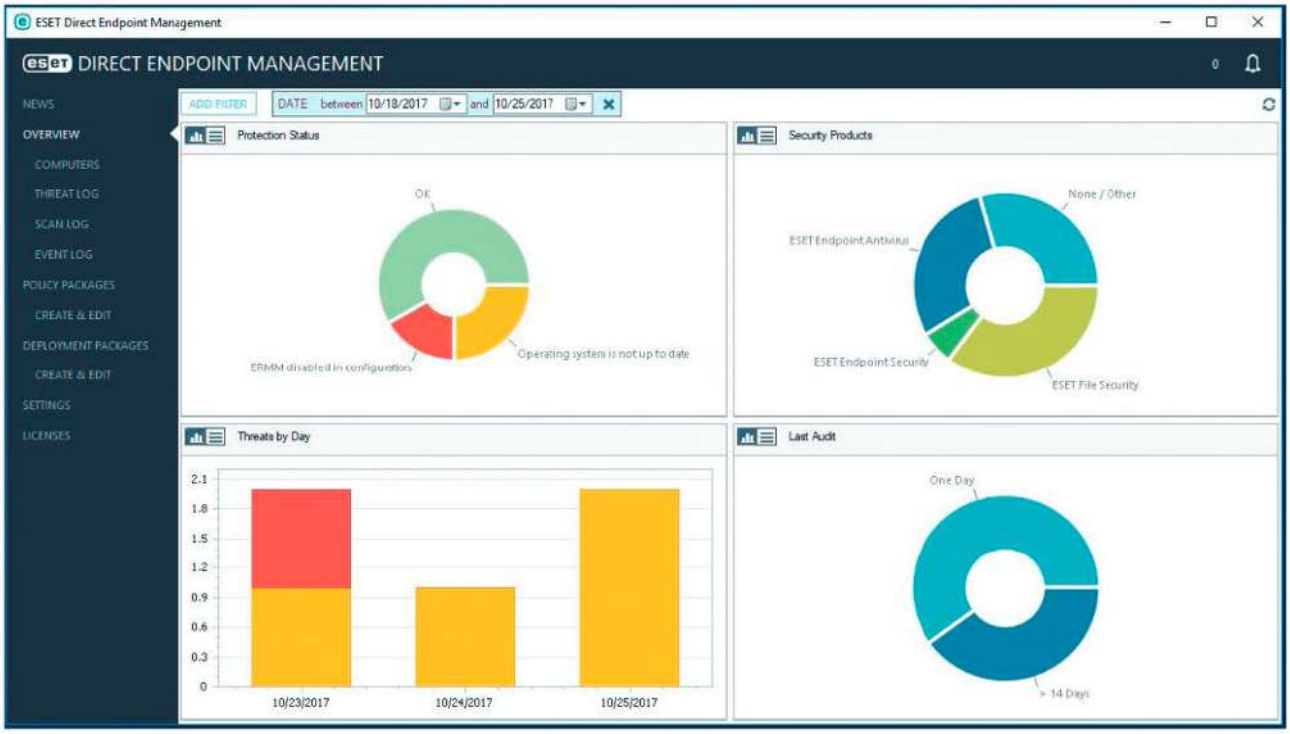
- Oberste Vorsicht bei Malwarefunden. Meldet ein Malwarescanner einen Zwischenfall, sollte dem immer nachgegangen werden und zwar so schnell wie möglich. Handelt es sich um einen Fehlalarm, will der Nutzer schnellstmöglich weiterarbeiten. Handelt es sich um eine echte Bedrohung, sind Folgemaßnahmen wie Rechnerquarantäne unverzüglich zu realisieren.

- Augen auf beim Hardwarezustand. Überprüfen Sie regelmäßig den Zustand Ihrer Systeme. Es gibt Tools, die erkennen, wenn eine Festplatte kurz davor ist, den Dienst zu verweigern. Sie sollte also möglichst vor dem Ausfall getauscht werden.- Internetzugang am Firmenstandort. Ist dieser gestört oder sinkt die Bandbreite, behindert das auch das Arbeiten vom Home-Office aus. Setzen Sie also Schwellwerte, um schnellstmöglich reagieren zu können.

Weitere Informationen

Anderweitige Informationen bezüglich der Mitarbeiter, bei denen Heimarbeit nicht möglich ist, sowie aktuelle Informationen zu möglichen Soforthilfen finden Sie auf den Webseiten der IHK, des BVMW und Ihrer jeweiligen Landesregierungen.

Sollten Sie mit der Situation und den untenstehenden Handlungsempfehlungen an Grenzen stoßen, egal ob personell oder des Verständnisses, wenden Sie sich am besten an spezialisierte, kompetente Dienstleister wie Managed Services Provider.



5 TIPPS FÜR EIN SICHERES HOME-OFFICE

1 Antiviren-software einsetzen

Nutzt eine moderne Internet Security-Suite. Neben einem Virenschutz sollte die Sicherheitslösung auch einen Ransomwareschutz, eine Firewall, ein Banking- und Shopping-Schutz, ein Diebstalschutz sowie ein Filter für Spam- und Phishing-Mails enthalten.

2 Betriebssystem aktualisieren

Aktualisiert Euer Betriebssystem und die verwendete Software. In der Regel aktualisieren sich viele Programme sowie das Windows-Betriebssystem automatisch. Regelmäßiges updaten schützt vor gefährlichen Sicherheitslücken.

3 2-Faktor-Authenitifizierung nutzen

Nutzt die sogenannte 2-Faktor-Authentifizierung bei Facebook, Twitter, Instagram und Euren anderen Lieblingsseiten – und Accounts. Dieser Service ist kostenlos und kinderleicht einzurichten. Neben dem Passwort gibt es dadurch eine weitere Schutzebene, zum Beispiel durch einen Einmal-Code.

4 Verschlüsselung aktivieren

An einer guten Verschlüsselung beißen sich Cyberkriminelle die Zähne aus! So bleiben Eure Daten auch im Fall der Fälle vor fremden Augen geschützt. Idealerweise verschlüsselt Ihr Euren gesamten Rechner - dazu gibt es Windows-Bordmittel und sogar kostenfreie Spezialprogramme.

5 VPN-Verbindung einrichten

VPN-Lösungen erstellen verschlüsselte Kommunikations-tunnel" zwischen Eurem PC und dem Unternehmens-netzwerk. Die gesendeten Daten bleiben so vor neugierigen Blicken verborgen. Gefährliche Man-in-the-Middle-Angriffe verpuffen wirkungslos.

SO MACHEN SICH UNTERNEHMEN FIT FÜR DAS HOME-OFFICE

PLANUNG IST TRUMPF

Behalten Sie den Überblick

- Notbesetzung IT-Abteilung festlegen
- IT-Ausrüstung komplettieren
- Inventarliste anfertigen
- Zusätzliche Software-Lizenzen einkaufen
- Anleitungen/Tutorials für Anwender erstellen

(VPN)-ZUGÄNGE VORBEREITEN

Trau schau wem

- VPN-Verbindungen einrichten
- Alternativ RDP-Verbindungen vorbereiten
- Zugänge für Online-Services individuell bereitstellen

HARDWARE VORBEREITEN

Gut gerüstet geht es einfacher

- Notebooks aktualisieren, ggf.aufrüsten
- Monitore, Tastaturen, Mäuse etc.bereitstellen
- Fernwartungs-Software / MDM auf allen Geräten installieren

BACK-UP UND SYSNCRONISATION

Datensicherung ist Trumpf

- Back-Ups Compliance-konform erstellen
- Daten synchronisieren, damit sie lokal und im Netzwerk vorliegen
- Kopien vor Ransomware schützen

IT-SECURITY UMSETZEN

Mit Sicherheit besser arbeiten

- Virenschutz aktualisieren
- Betriebssystem und eingesetzte Software aktualisieren
- 2-Faktor-Authentifizierung aktivieren
- Datenverschlüsselung einschalten

AN MULTI-FAKTOR-AUTHENTIFIZIERUNG KOMMT NIEMAND VORBEI

Passwort weg, Daten futsch, Ärger groß: Hacker haben freie Bahn, wenn sie an sicher geglaubte Zugangsdaten gelangen – und im schlimmsten Fall bleibt dies lange Zeit unerkannt. Unternehmen sollten sich mit einer Multi-Faktor-Authentifizierung davor absichern. Erst recht, wenn sie ihre Mitarbeiter während der Corona-Krise ins Home-Office schicken.

Die Coronavirus-Pandemie und die damit einhergehenden Schutzmaßnahmen der Regierung stellen Unternehmen vor neue Herausforderungen. Selbst Firmenlenker, die sich bisher strikt gegen Home-Office entschieden haben, müssen in der aktuellen Situation dezentrales Arbeiten auf einmal ermöglichen, um weiterhin am Markt bestehen und Mitarbeiter schützen zu können.

„Unternehmen sind im Zuge der Corona-Krise gezwungen, in kürzester Zeit Home-Office- Arbeitsplätze einzurichten. Der geschützte Zugang zu sensiblen Daten und somit die sichere Anmeldung ist hier von existenzieller Bedeutung. Allein auf Passwörter als Zugangsschutz zu wichtigen Daten zu setzen, könnte sich als fatal herausstellen“, betont Thorsten Urbanski von ESET. Der Einsatz von VPN-Lösungen ist hier ebenso obligatorisch wie der Einsatz von Authentifizierungslösungen.

Unternehmen sollten daher die Zugänge zu ihrem Netzwerk und ihre IT-Dienstes effektiv absichern. Passwörter sind hier nur zweite Wahl.

Vom Home-Office ins Netzwerk gelangen: Nur mit Authentifizierung

Der Zugang zu den Cloud-Diensten und Firmenservern muss dabei selbstverständlich sicher erfolgen. Nichts wäre schlimmer, als dass Unbefugte im Netzwerk ihr Unwesen treiben. Experten sind sich einig: Der klassische Weg mit Benutzername plus Passwort allein reicht als Schutzmaßnahme nicht mehr aus. Das bestätigt auch Microsoft selbst. Allein im Januar dieses Jahres wurden rund 1,2 Millionen Microsoft-Benutzerkonten gehackt, wie der Konzern auf einer Sicherheitskonferenz bekannt gab. Die Microsoft-IngenieurInnen erklärten auch, warum diese Konten so unsicher sind: 99,9 Prozent der kompromittierten Konten verwenden keine Multi- Faktor-Authentisie-

rung (MFA), bei der zum Beispiel neben einem Passwort auch ein Fingerabdruck- oder Gesichts-Scan eingesetzt wird.

An Auswahl geeigneter Lösungen mangelt es nicht. Auf dem Markt befindet sich bereits eine Reihe von Lösungen mit unterschiedlichen Ansätzen. Diese variieren nicht nur im Anschaffungspreis, sondern auch im späteren Administrationsaufwand. Als Authentifizierungsverfahren werden auf vielen Geräten Smartcards, OTP Tokens, Biometrie via Fingerprint und Venenleser, RFID Tokens, X.509 Zertifikate, QR Codes und USB-Dongles eingesetzt. Letztere erweisen sich als besonders einfach. Der Anwender muss dann keine Installationen, Anpassungen oder Änderungen auf dem verwendeten Rechner vornehmen, sondern lediglich den USB-Dongle einstecken. Noch einfacher gelingt die Absicherung mit softwarebasierten Lösungen wie ESET Secure Authentication. Diese nutzt eine App für gängige Smartphones, in der ein Einmalcode generiert wird. Dieser muss zwingend zur korrekten Kombination aus Benutzername und Passwort zusätzlich eingegeben werden. In der aktuellen Corona-Krise stellt der Hersteller die Software kostenlos zur Verfügung unter https://www.eset.com/de/sicheres-home-office/

Passwörter als Gefahrenquelle

Das Grundproblem, das dahintersteckt, ist so einfach wie folgenreich: Ohne Zugangscodes läuft nichts mehr in der modernen IT. Der Login in E-Mail- Konten, Cloud-Services oder Firmennetzwerke erfordert aus Sicherheitsgründen immer die Kombination aus Benutzername und Passwort. Trotz aller bahnbrechenden Entwicklungen in den letzten Jahrzehnten dient das „Urgestein Passwort" immer noch in seiner ursprünglichen Form als Zugangskontrolle - oftmals sogar als einzige und nicht ausreichende Authentifizierungsmöglichkeit.

Eigentlich sollen Passwörter den Zugang zu sensiblen Daten oder Zugängen absichern. In der Praxis sind sie jedoch oftmals schlecht gewählt. Statische Passwörter können beispielsweise abgefangen oder im Darknet erworben werden. Benutzerdefinierte Zugangsdaten sind selten stark genug definiert und durch intelligente Wörterbuchattacken, Brute-Force-Methoden oder simples Raten einfach zu überwinden.

Viele Anwender nutzen sogar identische Passwörter im dienstlichen und privaten Bereich. Letztlich werden Passwörter – wegen der schlechten Merkbarkeit und den jeweiligen betrieblichen Anforderungen - nicht zufällig generiert. Oftmals beinhalten sie einfach zu knackende Charakteristika wie Name, Geburtstag und fortlaufende Nummerierungen.

In vielen Unternehmen ist die Praxis, alle 90 Tage Passwörter zu wechseln, fest verankert. Das führt aber letztendlich nicht zu mehr Sicherheit, sondern nur zu einer Vermischung von privaten bzw. geschäftlichen Zugangsdaten und somit zu unsicheren IT-Systemen. Nicht von ungefähr hat das Bundesamt für Sicherheit in der Informationstechnik (BSI) genau diese Empfehlung in seinem aktuellen ITGrundschutz- Katalog ersatzlos gestrichen. Geraten Passwörter ohne weitere Absicherung in falsche Hände, haben Cyberkriminelle freie Fahrt.

Richtig unangenehm und teuer wird es für Unternehmen dann, wenn dabei gegen die Datenschutzgrundverordnung (DSGVO) verstoßen wird. Der DSGVO ist es egal, wenn Unternehmen Daten verlieren, solange sie sich damit nur selbst schaden. Wer jedoch Kunden- oder Patientendaten oder auch Informationen über die eigenen Mitarbeiter „verliert", weil sie nicht ausreichend geschützt sind, setzt womöglich die Existenz seines Unternehmens aufs Spiel.

Multi-Faktor-Authentifizierung verstärkt Zugangssicherheit

Wer sich mit seinem dienstlich gelieferten Gerät - beispielsweise dem Notebook, dem Tablet oder dem Smartphone - in ein Firmennetzwerk, einen Cloud-Service oder Online-Dienst einwählt, benötigt in den meisten Fällen nur ein gültiges Passwort in der Zugangssoftware.

Dieses Verfahren erfüllt längst nicht mehr die Anforderungen moderner IT-Sicherheit. Das BSI, Cyber-Abwehrexperten und IT-Security-Forscher empfehlen daher die sogenannte Multi-Faktor- Authentifizierung (MFA). Sie nutzt die Kombination von zwei oder mehr Berechtigungsnachweisen zur Prüfung der Identität.

Dazu zählen beispielsweise spezielles Wissen, biometrische Merkmale oder zusätzliche Hardware (z.B. Token, Security Keys). Die Kombination aus zwei oder mehr dieser voneinander unabhängigen Faktoren sichern Anmeldeverfahren stärker ab.

Dennoch bleibt ein Problem: Kleinere Unternehmen besitzen nur selten die finanziellen Mittel und personellen Ressourcen dafür. Auch Administratoren größerer Netzwerke tun sich schwer, denn die stetig steigende Anzahl an mobilen Geräten sorgt für mehr Arbeit und Kosten. Hinzu kommt, dass der Anwender die zweite Sicherung komfortabel bedienen können muss. Je komplizierter das Verfahren ist, desto mehr wird die Durchsetzung von Systemen zur Absicherung der IT behindert.

Moderne Zugangskontrolle mit ESET Secure Authentication

Eine interessante Alternative für Unternehmen, die die Zugangskontrolle auf eigene Netzwerke oder Dienste unkompliziert selbst administrieren wollen, bietet der slowakische Antivirenhersteller ESET mit „ESET Secure Authentication" (ESA) an. Die softwarebasierte Lösung zur Multi-Faktor- Authentifizierung ebnet einen sicheren Zugang zu Online-Anwendungen und Netzwerkumgebungen. Mit ESA lassen sich sogar komplett passwortlose Umgebungen schaffen: Dank Integration von Windows Hello oder FIDO-basierter Hardware kann bereits das Windows Login passwortlos durchgeführt und abgesichert werden.

Mit ESET Secure Authentication sind Unternehmen jeglicher Größe in der Lage, mobile Devices sicher einzusetzen, Datenschutzvorfälle zu vermeiden und selbst strengste Compliance-Anforderungen zu erfüllen. Mithilfe der leistungsstarken und intuitiven Multi-Faktor-Authentifizierung per Smartphone, Smartwatch oder bestehender Hardwaretoken ist der Einsatz zugleich äußerst koste ffizient - ohne dabei Security-Kompromisse eingehen zu müssen.

Die aktuelle ESA-Generation enthält eine Reihe neuer Technologien und Features, darunter eine passwortlose Anmeldung und die Unterstützung der biometrischen Authentifizierung in der mitgelieferten App. Dank der Unterstützung von Windows, macOS und Linux ist die Implementierung in heterogene Netzwerkumgebungen problemlos möglich. Gleichzeitig ist sie einfach zu installieren und zu verwalten. Das mitgelieferte Software Development Kit (SDK) und die API ermöglichen optimale Integrationsflexibilität für einen umfassenden Schutz von Anwendungen und Daten.

Passwortlose Anmeldungen

Das Auslaufmodell „Benutzername plus Passwort" ist vielen Unternehmen ein Sicherheits-Dorn im Auge. Sie setzen immer mehr auf Authentifizierungsmethoden, mit denen sie ganze Umgebungen ohne Passwörter absichern können. Dies geschieht mithilfe von FIDO 2.0 kompatibler Hardware (z.B. Sticks) oder Windows Hello – beides unterstützt ESET bereits ab dem Windows Login. Erstmals können auch biometrische Verfahren in ESA eingebunden und über die Konsole verwaltet werden.

Sicher in die Cloud

Neben der Absicherung von Anwendungen vor Ort kann ESET Secure Authentication zum Schutz von Web- und Cloud-Diensten wie Microsoft Office 365, Google Apps, Dropbox und viele weitere durch ADFS 3.0 oder SAML Protokoll Integration eingesetzt werden. Letzteres kann über verwendete Identity Provider diverse SingleSignOn-Varianten für viele weitere Anwendungen, Dienste und Plattformen anbieten – ohne, dass auf das von ESET bereitgestellte SDK zurückgegriffen werden muss.

Multi-Faktor-Authentifizierung via Biometrie

Auch die neueste Version der ESA-App kann nun mit den Smartphone-eigenen Authentifizierungsoptionen (Touch ID, Face ID oder Android Fingerprint) genutz werden. Damit schlagen Unternehmen zwei Fliegen mit einer Klappe: Sie erweitern ihre biometrische Authentifizierung um einen weiteren Faktor, der ebenfalls ohne Passwort auskommt.

Starke Performance auch für Enterprise

ESET Secure Authentication kann nun – abhängig vom Installationstyp (gebunden an die Microsoft Active Directory oder Stand Alone) - pro Instanz bis zu 20.000 Seats und 80 Anfragen pro Sekunde verarbeiten. Die Einbindung eigener SQL-Server und der Betrieb mehrerer Instanzen macht die Lösung flexibel einsetzbar und somit auch für Enterprise- Kunden interessant. Mit Secure Authentication stellt ESET eine erweiterte Zugangskontrolle für VPN-Verbindungen, Outlook Web App, Microsoft Sharepoint, Dynamics DRM sowie Remote Desktop Verbindungen vor. Sie unterstützt die Compliance-Vorgaben vieler Staaten. Dazu zählen unter anderem PCI/DSS, FFIEC, Sarbanes Oxley, NIST, IS Standards oder HIPAA. Die Sicherheitslösung besitzt einen nativen Support für Exchange Server 2013 und VMware Horizon View. Dank der RADIUS-Unterstützung und der API kann nahezu jede marktübliche VPN-Appliance um diese Authentifizierungsfunktionen erweitert werden.

Remote Management

ESET Secure Authentication verwendet eine eigens entwickelte Managementkonsole, die über einen Webbrowser zugänglich ist. Die Anwender können sich für die Integration mit Active Directory entscheiden, die Lösung aber auch in Nicht-ADUmgebungen einsetzen. Nach der Installation sind für die Einrichtung und Bereitstellung von ESET Secure Authentication keine zusätzlichen Schulungen oder professionellen Dienstleistungen erforderlich.

Setup in nur 10 Minuten

ESA kann auch in kleinen Unternehmen ohne eigene IT-Abteilung problemlos auf- und eingesetzt werden. Unabhängig von der Firmengröße beansprucht die Installation dank der Möglichkeit, mehrere Nutzer gleichzeitig einzurichten, nur wenig Zeit.

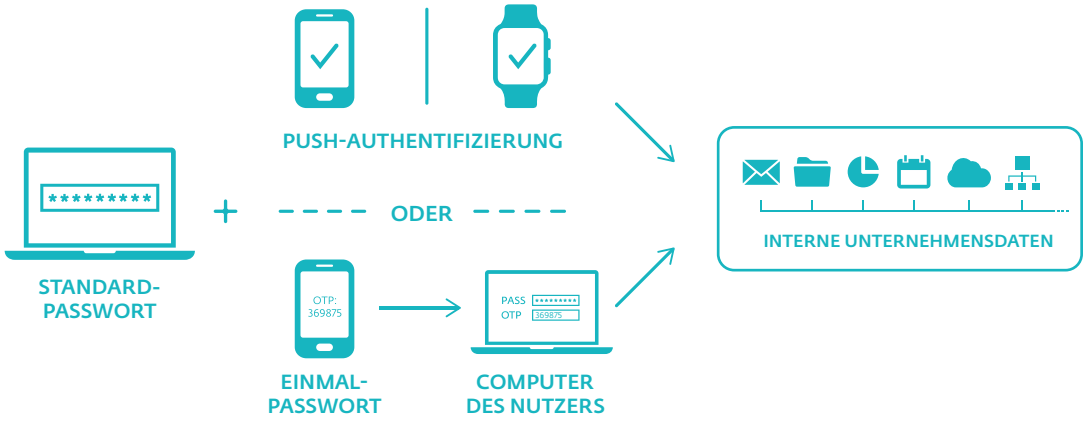
Keine zusätzliche Hardware nötig

ESET Secure Authentication erfordet keine zusätzliche Hardware. Nach der Installation der 10MB-großen Anwendung auf dem Server können Administratoren umgehend mit der Bereitstellung starten.

Fazit

Das Passwort hat als alleinige Zugangskontrolle längst ausgedient. Geht es verloren, haben Unbefugte nahezu alle Möglichkeiten, bestmöglichen Profit daraus zu schlagen. Die Multi-Faktor- Authentifizierung setzt sich immer mehr durch, denn sie erhöht die Sicherheit der Zugangskontrolle immens. Dabei muss es dem Anwender so einfach wie möglich gemacht werden, umso schneller wird sich die Authentifizierungsmöglichkeit im digitalen Leben und beruflichen Alltag etablieren.

Gerade jetzt während der Corona-Pandemie, wo so viele Menschen im Home-Office arbeiten, wäre es der ideale Zeitpunkt, den Übergang zur Multi-Faktor-Authentifizierung zu vollziehen.Lösung im Einsatz, überprüfen Sie ebenfalls, ob die ursprüngliche Lizenzgröße noch ausreicht.



SECURE AUTHENTICATION

SITUATION

Die Mitarbeiter eines Unternehmens sind unzufrieden mit den strengen Passwortregeln. Sie kritisieren, dass sie sich alle drei Monate ein neues, kompliziertes Kennwort ausdenken und merken müssen. Manche Kollegen kleben ihre Zugangsdaten auf Zetteln an ihren Laptop – für das Unternehmen ein großes Sicherheitsrisiko. Der IT- und Datenschutzverantwortliche empfiehlt, mit einer Multi-Faktor-Authentifizierungslösung unsicheren Passwortmethoden ein Ende zu setzen.

UND JETZT?

Die Multi-Faktor-Authentifizierung sollte für die Mitarbeiter so bedienbequem wie möglich sein und bestehende Prozesse nicht unnötig kompliziert machen. Zudem darf die Lösung das IT-Budget nicht überstrapazieren. Ideal wäre eine Software-Lösung, die sich mit den Firmen-Smartphones nutzen lässt. Das hieße nämlich, dass sich ein Mitarbeiter weder auf neue Tools einlassen noch das Unternehmen zusätzliche Hardware anschaffen müsste.

ESET HAT DIE LÖSUNG – 3 Gründe für ESET Secure Authentication

SICHERER LOGIN PER KNOPFDRUCK

ESET Secure Authentication sichert Zugänge mit einem zusätzlichen Faktor, ohne Nutzer zu überfordern. Die bequemste Bereitstellungsmöglichkeit funktioniert über eine Push-Nachricht aufs Handy des Mitarbeiters, die er einfach per Fingerabdruck bestätigt.

SAMTWEICHE EINBINDUNG

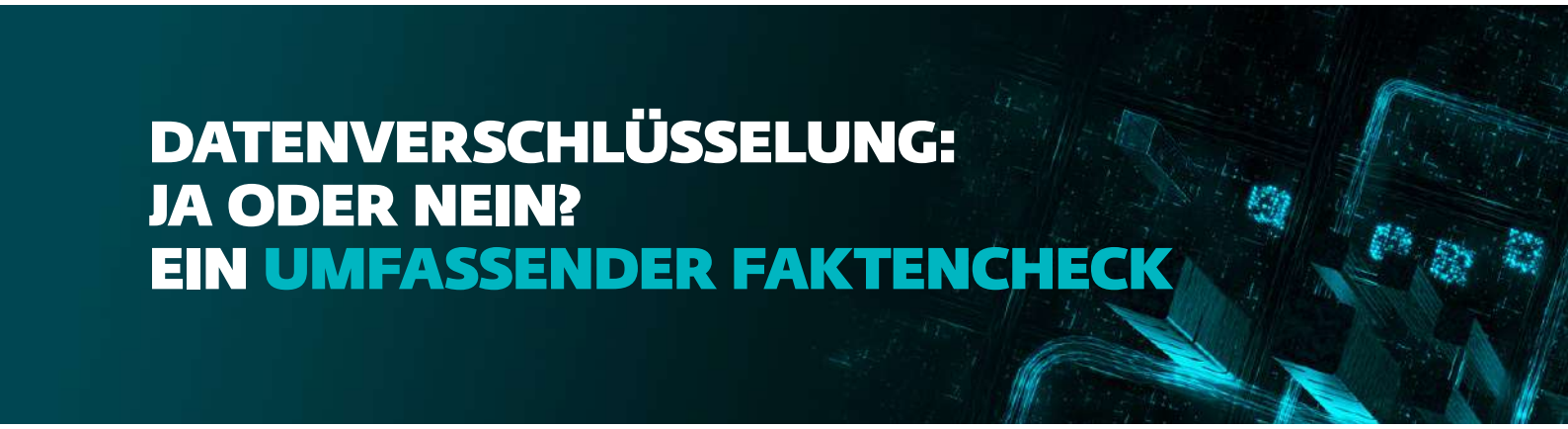
Die Lösung unterstützt alle iOS und Android Smartphones und lässt sich mit den geräteeigenen biometrischen Verfahren nutzen. Auch FIDO-basierte Sticks und andere Token werden problemlos unterstützt. Zusätzliche Hardware-Anschaffungen sind also nicht notwendig.

PASSWORTLOSE ANMELDUNGEN

Bedienbequem muss es sein: Passwortlose Umgebungen per SingleSignOn lassen sich dank der Unterstützung des SAML-Protokolls in die Praxis umsetzen. Mit der Integration von Windows Hello und FIDO-basierter Hardware sind auch passwortlose Windows Logins möglich.

Die wichtigsten Eigenschaften in Kürze:

- Große Flexibilität in puncto Lizenzform, Authentifizierungmethodik, Hardwareeinsatz und Anforderungen an die Infrastruktur
- Vielfältige Authentifizierungsmöglichkeiten: Push-Benachrichtigung, Einmal-Passwort via App, SMS oder Token sowie individuelle Methoden
- Unterstützt die biometrischen Authentifizierungsverfahren eingesetzter Smartphones (Android und iOS)
- Schütz Windows und Server Logins, Cloud- und Webanwendungen wie Google App, Office 365 oder Dropbox, RDP und VPNs
- Realisierung von passwortlosen Umgebungen via SingleSignOn dank Unterstützung des SAML-Protokolls
- Whitelisting von IP Bereichen und bestimmten Applikationen zum Finetuning der MFA



DATENVERSCHLÜSSELUNG: JA ODER NEIN? EIN UMFASSENDER FAKTENCHECK

Deutsche sind laut einer Umfrage des europäischen Security-Herstellers ESET Verschlüsselungsmuffel. Dies hat sich seit der Einführung der Datenschutzgrundverordnung in 2018 nur leicht verbessert. Neue Impulse erhält die Diskussion durch die Corona-Krise und der einhergehenden Verlagerung der Geschäftstätigkeit vieler Angestellten ins Home-Office. Denn auch dort müssen betriebliche Informationen sicher vor fremden Blicken geschützt sein.

Was könnte ein Unternehmen mit 20 Millionen Euro anstellen? Aufgeschobene Investitionen nachholen, das Bürogebäude modernisieren oder das Gehalt der eigenen Angestellten aufstocken. Oder – wie ein großes deutsches Internet-Unternehmen – als Bußgeld an nationale Aufsichtsbehörden wegen Verstößen gegen die Datenschutzgrundverordnung (DSGVO) entrichten. Damit steht der Beklagte nicht allein da: Seit Inkrafttreten der Datenschutzgrundverordnung im Mai 2018 wurden bisher 160.000 Verstöße gemeldet und geahndet. Die chtsanwaltskanzlei DLA Pieper beziffert den Gesamtwert der Strafen auf 114 Millionen Euro.

Die Gründe der vielen Verfehlungen sind vielfältig. Letztlich wurde eine elementare Frage nur rudimentär beantwortet: Wie kann man die digitalen Schätze zum Wohle aller schützen und vor allem datenschutzrechtlich korrekt durchführen? Vom Prinzip her gibt es nur drei Möglichkeiten. Entweder man schließt den Zugang zu den Daten bombensicher ab oder man verschlüsselt sie. Idealerweise macht man beides. Leider gescheh alle drei Varianten zu selten. Ansonsten würden nicht laufend lange Listen – unverschlüsselt - mit Benutzernamen plus Passwort oder Kreditkartennummern inklusiv Kennziffern gestohlen werden - und dann im Darknet kursieren, verkauft und von Kriminellen eingesetzt werden. Der Dumme ist letztlich der Anwender, der seine Daten einem Unternehmen anvertraut hat. Und dies im guten Glauben, dass sie dort sicher seien wie Gold in Fort Knox. Eine Verschlüsslung setzen fast alle Anwender voraus und werden oftmals bitter enttäuscht. Dabei spielt es offensichtlich keine Rolle, ob es sich beim Datenspeicher um einen Großkonzern oder einen Gewerbetreibenden handelt.

Vielleicht findet bei den großen Sündern bereits ein Umdenken statt. Denn ethisches Handeln, vor allem beim Thema „Datenverarbeitung" und Nutzung, wird für Menschen/Kunden/Anwender immer wichtiger.

Wie die Frankfurter Allgemeine Zeitung treffend feststellte, ist Datenschutz ein Menschenrecht. Immer mehr Personen sehen genau das als wichtige Prämisse. Parallel zum Thema „Nachhaltigkeit" in der Konsumgesellschaft wächst auch das menschliche Bedürfnis nach Datensicherheit stetig. Und die Verschlüsselung gehört als elementarer Bestandteil dazu. Dies gilt vor allem für betriebliche Informationen – unabhängig davon, ob sie im Büro oder im Home-Office bearbeitet werden.

JURISTISCHE FRAGEN

Muss überhaupt verschlüsselt werden? Grundsätzlich besteht kein Muß zur Verschlüsselung. Die gültige Datenschutzgrundverordnung nimmt aber Organisationen in die Pflicht, personenbezogene Daten angemessen zu schützen. Im Erwägungsgrund 83 der DSGVO – „Sicherheit der Verarbeitung" – sind die Anforderungen klar definiert:

„Zur Aufrechterhaltung der Sicherheit und zur Vorbeugung gegen eine gegen diese Verordnung verstoßende Verarbeitung sollte der Verantwortliche oder der Auftragsverarbeiter die mit der Verarbeitung verbundenen Risiken ermitteln und Maßnahmen zu ihrer Eindämmung, wie etwa eine Verschlüsselung, treffen. Diese Maßnahmen sollten unter Berücksichtigung des Stands der Technik und der Implementierungskosten ein Schutzniveau – auch hinsichtlich der Vertraulichkeit – gewährleisten, das den von der Verarbeitung ausgehenden Risiken und der Art der zu schützenden personenbezogenen Daten angemessen ist.

Bei der Bewertung der Datensicherheitsrisiken sollten die mit der Verarbeitung personenbezogener Daten verbundenen Risiken berücksichtigt werden, wie etwa – ob unbeabsichtigt oder unrechtmäßig – Vernichtung, Verlust, Veränderung oder unbefugte Offenlegung von oder unbefugter Zugang zu personenbezogenen Daten, die übermittelt, gespeichert oder auf sonstige Weise verarbeitet wurden, insbesondere wenn dies zu einem physischen, materiellen oder immateriellen Schaden führen könnte."

Eine Maßnahme, die ausdrücklich in Artikel 32 zur Sicherheit der Verarbeitung personenbezogener Daten genannt wird, ist die Verschlüsselung. Sie wird als geeignete technische Maßnahme empfohlen und anerkannt. Wenn Angreifer alle Hürden wie Firewall, Antiviren-Software oder weitere Sicherungslösungen überspringen, ist eine gute Verschlüsselungslösung das letzte Bollwerk. Sie sorgt dafür, dass nach einem Datendiebstahl Cybergangster zumindest keinen Profit aus den Informationen ziehen können – und die Vertraulichkeit der Daten bewahrt bleibt.

Wer glaubt, auch ohne Verschlüsselung am Markt agieren zu können, für den hält die DSGVO eine Fülle von Anforderungen und verschärfte Strafandrohungen bereit. Und die haben es in sich: Wenn es zu einer Datenschutzpanne kommt, sind saftige Bußgelder fällig, die sogar die Existenz eines Unternehmens gefährden können.

Auch das Bundesdatenschutzgrundgesetz (BDSG) trifft klare Aussagen, wie mit vertraulichen Daten zu verfahren ist. Paragraph 64 BDSG (neu) – „Anforderungen an die Sicherheit der Datenverarbeitung" – geht ins Detail und fordert:

- Verhinderung des unbefugten Lesens, Kopierens, Veränderns oder Löschens von Datenträgern (Datenträgerkontrolle)
- Verhinderung der unbefugten Eingabe von personenbezogenen Daten sowie der unbefugten Kenntnisnahme, Veränderung und Löschung von gespeicherten personenbezogenen Daten (Speicherkontrolle)
- Gewährleistung, dass die zur Benutzung eines automatisierten Verarbeitungssystems Berechtigten ausschließlich zu den von ihrer Zugangsberechtigung umfassten personenbezogenen Daten Zugang haben (Zugriffskontrolle)

Die Verschlüsselung erscheint vor diesem Hintergrund als effektivste und effizienteste Maßnahme. Sicherlich bieten sich für die Umsetzung der Punkte auch andere Maßnahmen an. Diese dürften aber mehr zeitlichen Aufwand und finanzielle Mittel erfordern. Welche Auswirkungen hat es, wenn man nicht verschlüsselt? Wer den Zugang zu gespeicherten Informationen bombensicher gestaltet, kann auch ohne Verschlüsselung agieren. Doch wehe, wenn es schiefläuft: Neben dem Verlust der Daten (und damit vielleicht auch der Geschäftsgrundlage) drohen immense Strafen durch die Datenschutzgrundverordnung. Vom Image- und Reputationsschaden bei Kunden und Geschäftspartnern ganz zu schweigen.

Weitere Probleme kommen noch aus ganz anderer Richtung. Ein Beispiel: Ohne Verschlüsselung keine Cyberversicherung! Vermeintlich Pfiffige denken möglicherweise, sich teure Investitionen in Sicherheitstechnologien sparen zu können und stattdessen eine Cyberversicherung abzuschließen. Was hilft besser gegen Schäden durch Hacker und Kriminelle als eine Versicherungs-Police. Doch hier wird die Rechnung ohne den Wirt gemacht. Denn die Anbieter setzen Sicherheitsstandards voraus, die der Leistungsnehmer erbringen muss. Und genau in diesen Punkt spielt die Verschlüsselung – oft in Verbindung mit der Zugangskontrolle durch Zwei- Faktor-Authentifizierung – eine entscheidende Rolle. Ohne diese Schutzmaßnahme bleibt der Kunde wohl auf seinem Schaden sitzen, sofern ein Vertrag überhaupt zustande kommt.

Wer hingegen seinem umfassenden Sicherheitssystem die Krone aufsetzen möchte, der liegt mit einer Cyber-Police richtig. Dies sichert die Restrisiken ab und macht zumindest die finanzielle Seite IT-bedingter Ausfälle erträglich.

FRAGEN AUS DER PRAXIS

Warum wird oftmals nicht verschlüsselt?

Unter vielen Antworten hören Experten eine sehr oft: „Ich habe Angst, dass ich den digitalen Schlüssel verliere und nicht mehr an meine Daten komme." Tatsächlich war das in der Vergangenheit ein großes Problem insbesondere für Gewebetreibende und kleinere Betriebe. Sie widmeten ihre Zeit lieber Kunden und Klienten als der Technik. Doch dieses ist bereits benutzerfreundlich und dennoch sicher gelöst worden. Die unnötige Furcht, die besonders bei eher wenig technisch versierten Anwendern vorherrscht, hält sich hartnäckig.

Im Unternehmensumfeld spielt dies nur eine untergeordnete Rolle. Hier stellt sich eher die Verfahrensfrage, wie man Daten so verschlüsselt, dass nur eine berechtigte Gruppe der Anwender darauf zugreifen kann. Mit zunehmender Netzwerkgröße an Personal und Daten potenziert sich nämlich das Problem des Schlüsselmanagements. So darf beispielsweise die Personalabteilung per se nicht auf Vertriebsdaten zugreifen. Aber wenn das Gehalt und der Bonus eines Vertriebsmitarbeiters berechnet werden muss, ist der Zugriff sehr wohl wichtig. Nicht nur für den/die eigentliche Sachbearbeiter(in), sondern auch für deren Vertretungen bei Abwesenheit. Schon müssen Ausnahmen erstellt werden, die aber nur in bestimmten Fällen zum Tragen kommen. Man kann sich vorstellen, wie kompliziert sich dies in Netzwerken mit vielen Teilnehmern aus unterschiedlichen Abteilungen ausgestaltet. Dabei sind die Vorgaben durch die Datenschutzgrundverordnung noch nicht einmal berücksichtigt.

Logischerweise gehen viele Unternehmen dazu über, nur einen Teil der gespeicherten Informationen zu verschlüsseln. So lässt sich der Arbeitsaufwand begrenzen und dennoch ein gesundes Maß an Sicherheit herstellen. Hier liegt die Kunst eher darin,

die richtigen Daten zu codieren und den berechtigten Personen zuzuordnen. Selbstverständlich gibt es bereits Lösungen, die alles automatisch verschlüsseln und dies mit der Rechtevergabe durch Microsoft Active Directory koppeln. Mit letzterer umgeht man die Zuordnung der Rechte hatte zu jedem Benutzer. Doch das hat seinen Preis: Wenn jede benutzte Datei ständig ent- und verschlüsselt wird, erzeugt das eine enorme Netzwerklast. Die dafür benötigten Ressourcen von Hardware bis zum Stromverbrauch treiben die Kosten in ungeahnte Höhen.

Was ist wichtiger, Datenträgerverschlüsselung oder Datenverschlüsselung?

Keine ist wichtiger. Hauptsache, es wird überhaupt verschlüsselt. Eine Datenträgerverschlüsselung sollte auf jeden Fall auf mobilen Geräten Pflicht sein. 3.300 Laptops gehen allein an europäischen Flughäfen verloren – wöchentlich. Damit zählt der mobile Rechner zu den Top 10 der am meisten verloren gegangenen Dinge. Und das nur knapp hinter Sonnenbrille und Schlüsselbund.

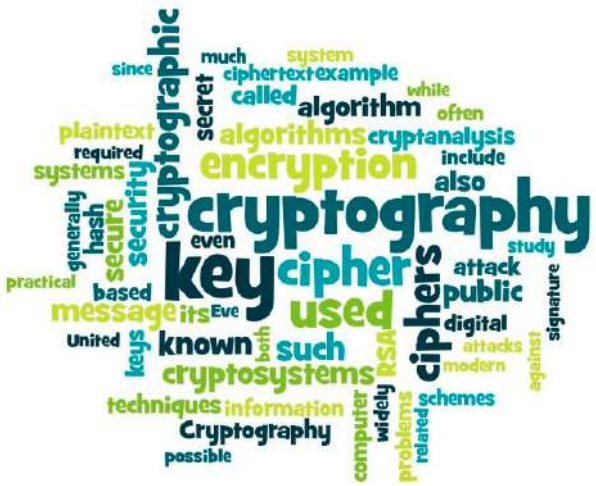
Der physische Verlust des Geräts ist für seine Besitzer in erster Linie ärgerlich. Auf den zweiten Blick entsteht für Selbstständige wie auch für Unternehmen ein sehr ernstes Problem. Außer den Kosten für eine Neuanschaffung droht auch das Abhandenkommen von wertvollem Know-how, wichtigen Betriebsinformationen, Zugängen zu Netzwerken und Konten oder sogar Kundendaten. Die Folgen können verheerend sein.

Nicht nur personenbezogene Daten (als Massenware) sind von hohem Wert. Besonders der Schutz „digitaler" Güter wie Know-how und Expertise, Geschäftsgeheimnisse wie Patente und Pläne und aber auch simple Planungsdaten unterliegen in den seltensten Fällen einem ausreichendem Schutzkonzept.

Der große Vorteil der Datenträgerverschlüsselung liegt in der einfachen Bedienbarkeit. Produkte wie ESET Full Disk Encryption lassen sich in wenigen Minuten installieren und ins Netzwerk integrieren. Für den Anwender verändert sich quasi nichts: Er muss beim Booten des Geräts lediglich sein Benutzername und Kennwort eingeben – so, wie er es sowieso bislang machen sollte.

Welche Verschlüsselung ist denn überhaupt sicher?

Die richtige Verschlüsselung ist aktuell (und auch noch für eine recht lange Zeit) eine korrekt implementierte AES 256-Routine. Dieser Standard ist weltweit anerkannt und kann auch offiziell zertifiziert werden. Streng genommen erfreut sich AES 256 so großer Beliebtheit, dass sogar AES Instruktions-Sets in allen aktuellen CPUs enthalten sind oder sogar in der Hardware von Festplatten zum Einsatz kommt. Das führt neben der hohen Sicherheit dazu, dass der Speicher bei den Rechenoperationen kaum beeinträchtigt wird. Hinzu kommt, dass AES noch nie in der Praxis gehackt wurde. Es gibt bekannte Attacken, die aber nur unter „Laborbedingungen" mit Modellrechnungen vorgenommen wurden. Experten sind sich sicher, dass auch Quantencomputer, sollten sie denn mittelfristig auf den Markt kommen, vorerst nichts ändern werden.



Wie viele Hersteller gibt es in der Europäischen Union?

Der Markt an Verschlüsselungssoftware ist in den vergangenen Jahren stark gewachsen. Auch Hersteller aus der EU agieren erfolgreich am Markt. Doch nicht jeder nutzt eine selbst programmierte Lösung. Viele Anbieter verwenden Microsoft Bitlocker als Basis und veredeln diese nach ihren Vorstellungen.

Der Aspekt „Software aus Europa" ist zwischenzeitlich nicht nur aufgrund der Einhaltung des Anspruchs

von DSGVO-Konformität oder einem gewissen Qualitätsgedanken geprägt, sondern vermehrt auch aus Gründen der nationalen/ gefühlten Sicherheit. Unternehmen aus den USA z.B. unterliegen noch immer diversen Vorgaben (siehe Cloud Act, Privacy Act etc.), um Zugriff auf diverse Daten einzufordern. Das Vertrauen in nicht-europäische Unternehmen ist daher nicht uneingeschränkt gegeben und wird durch aktuelle politische Erfahrungen/Vorkommnisse weiter eingeschränkt. Nicht nur regierungsnahe Organisationen gehen verstärkt dazu über, Produkte von nicht europäischen Herstellern abzulösen.

SICHERHEITSTECHNISCHE FRAGEN

Kann Verschlüsselung vor Malware oder Ransomware schützen?

Nein. Vor Malware kann nur eine entsprechende Software schützen. Mit der Verschlüsselung der eigenen Daten kann der Anwender – egal ob privat oder dienstlich – lediglich verhindern, dass Fremde diese Informationen lesen und verarbeiten können. Aus dem erbeuteten „Datenwirrwarr" können Kriminelle keinen Profit schlagen. Je mehr Personen oder Unternehmen verschlüsseln, desto uninteressanter wird das zwielichtige Geschäftsmodell Datenklau und -verkauf. Und führen möglicherweise zu weniger Cyberangriffen mit dieser Zielvorgabe.

Bei Ransomware verhält sich die Sachlage etwas anders. Die Angreifer zielen nur darauf ab, Informationen selbst zu verschlüsseln und über eine Lösegeldforderung Geld zu erbeuten. Dabei spielt es keine Rolle, ob die Daten zuvor bereits codiert waren – am Inhalt sind die Kriminellen nicht interessiert. Auch hier kann nur eine wirksame Sicherheitslösung helfen, Verschlüsselung jedenfalls nicht. Aber schaden kann sie auch nicht.

Reicht die Verschlüsselung heutzutage aus?

IT-Verantwortliche sollten über den Tellerrand hinausschauen. Verschlüsselung sorgt nur für zusätzlichen Schutz, wenn sie auch genutzt wird. Und das wird sie nur, wenn die Bedienung die Mitarbeiter weder von der täglichen Arbeit abhält noch IT-Sicherheit komplizierter macht.

Die Krypto-Strategie eines Unternehmens sollte sich folglich nahtlos in das IT-Security-Konzept einfügen und die Compliance nicht unnötig aufblähen. Greifen Endpoint-Security, Zwei-Faktor-Authentifizierung und Verschlüsselung ineinander, entsteht eine ganzheitliche Sicherheitsstrategie, die Malware- Angriffe und Ausspäh-Aktionen verhindert und vertrauliche Firmendaten schützt.

Reicht die Windows-Anmeldung aus?

Nein, definitiv nicht. Die Windows-Anmeldung bietet weit weniger Sicherheit als vielfach gedacht. So mancher Windows-Anwender vertraut lieber einer trügerischen Sicherheit: Windows sei doch bei der Anmeldung durch die Eingabe von Benutzername und Passwort geschützt. Dummerweise dient sie weniger de m Schutz der Daten als vielmehr der Verwaltung der verschiedenen Benutzerprofile. Für halbwegs fortgeschrittene Anwender ist es ein Leichtes, über entsprechende Tools Zugriff zu erlangen oder gleich die gesamte Festplatte zu kopieren. Wenn man diesen Weg wählen möchte, ist eine Zwei-Faktor-Authentifizierung unabdingbar.

Sind Cyberversicherungen sinnvoll?

Aus unserer Sicht ist eine Cyberversicherung für Unternehmen sinnvoll, die mit sensiblen Daten arbeiten und ihr Geschäftsbetrieb von deren Verfügbarkeit abhängt. Sie tritt dann für Schäden ein, die im Zusammenhang mit Internetkriminalität entstehen. Nach einem Malware-Angriff zahlt der Versicherer beispielsweise für die Datenrettung oder kommt für die Kosten auf, die mit der vollständigen EDV-Wiederherstellung anfallen. Daneben garantieren die Anbieter weitere Hilfe, die meist als „Assistanceleistungen" ausgeschrieben sind.

Unternehmen sind gut beraten, sich die verschiedenen Vertragsbedingungen genau anzuschauen. Einfach eine möglichst günstige Versicherung abzuschließen, bedeutet nicht, dass alle Schäden einfach so ausgeglichen werden. Hier gilt es, im Vorfeld die passenden Bausteine auszusuchen, die wirklich abgesichert werden müssen. Je mehr die Versicherung leisten soll, desto teurer wird sie. Einem Irrtum unterliegt auch derjenige, der glaubt, dass die eigenen Anstrengungen und Investitionen in IT-Sicherheit verringert werden können. Genau das Gegenteil ist der Fall: Versicherungsnehmer sind gezwungen, den aktuellen Stand der Technik – auch in der IT-Sicherheit - einzusetzen. Dies kann unter Umständen bedeuten, dass investiert werden muss, bevor eine Police zum Abschluss kommt.

FULL DISK ENCRYPTION

SITUATION

Aufgrund seines Wachstums verarbeitet ein Unternehmen immer mehr personenbezogene Daten. Kunden, Mitarbeiter, Dienstleister – der Berg an Informationen wächst täglich höher. Aus diesem Grund hat sich das Unternehmen dazu entschlossen, auf Empfehlung der DSGVO eine Verschlüsselungslösung einzusetzen, um das Risiko für Datenpannen, Cyberangriffe und auch drohende Bußgelder zu minimieren.

UND JETZT?

Vor allem Mitarbeiter sollten die Verschlüsselungslösung bei ihrer täglichen Arbeit kaum „spüren". Sie muss einfach und zuverlässig sein, damit alle im Unternehmen nicht überfordert oder abgelenkt werden. Auch der Admin sollte in seinen beschränkten Kapazitäten eine möglichst unkomplizierte Lösung mit umfassenden Automatisierungsmöglichkeiten an die Hand bekommen, um nicht allzu viel Zeit in die Bereitstellung und Verwaltung investieren zu müssen.

ESET HAT DIE LÖSUNG – 3 Gründe für ESET Full Disk Encryption

STARKE VERSCHLÜSSELUNG LEICHT GEMACHT

Die eigens von ESET entwickelte Verschlüsselungslösung mit Pre-Boot Authentifizierung codiert zuverlässig gesamte Festplatten von Endpoints und lässt sich ganz bequem über das ESET Security Management Center oder den ESET Cloud Administrator verwalten.

OHNE PRODUKTTRAININGS LOSLEGEN

ESET Full Disk Encryption bedeutet sowohl für Nutzer als auch Admins einen absoluten Mehrwert bei minimalem Aufwand. Die Lösung ist innerhalb weniger Minuten aufgesetzt, spezielle Trainings oder Schulungen im Umgang sind nicht notwendig.

SECURITY MADE IN EU

Als europäischer Hersteller unterliegt ESET den Rechts- und Datenschutzvorschriften der EU. Diese rechtlichen und ethischen Grundsätze werden natürlich auch bei der Entwicklung der Lösungen eingehalten. So hilft EFDE Ihnen z.B. bei der Einhaltung der DSGVO.

Die wichtigsten Eigenschaften in Kürze:

- DSGVO-konforme Festplattenverschlüsselung mit Pre-Boot-Authentifizierung für Desktops, Notebooks und Tablets mit Windows Betriebssystem
- Verschlüsselung per Disk Encryption Treiber (256bit AES, via FIPS 140-2 validierter Windows Crypto API), TPM 2.0 oder Hardware (OPAL 2.0 kompatible Laufwerke)
- Einfaches Deployment und leichte Verwaltung über die Management-Konsolen ESET Security Management Center und ESET Cloud Administrator (bis 250 User)
- Bestmögliche Unterstützung im Support-Alltag (z.B. Passwortverlust der User)
- Erhältlich in Verbindung mit einer ESET Endpoint Lösung. Bestandskunden können EFDE ganz einfach zu Ihrer vorhandenen Lizenz hinzubuchen.

ESET ist ein europäisches Unternehmen mit Hauptsitz in Bratislava (Slowakei). Seit 1987 entwickelt ESET preisgekrönte Sicherheits- Software, die bereits über 110 Millionen Benutzern hilft, sichere Technologien zu genießen. Das breite Portfolio an Sicherheitsprodukten deckt alle gängigen Plattformen ab und bietet Unternehmen und Verbrauchern weltweit die perfekte Balance zwischen Leistung und proaktivem Schutz. Das Unternehmen verfügt über ein globales Vertriebsnetz in über 200 Ländern und Niederlassungen u.a. in Jena, San Diego, Singapur und Buenos Aires. Für weitere Informationen besuchen Sie www.eset.de oder folgen uns auf LinkedIn, Facebook und Twitter.

Folgen Sie ESET:

https://www.ESET.de

https://www.welivesecurity.de

https://twitter.com/ESET_de

https://www.facebook.com/ESET.DACH

CYBERSECURITY
EXPERTS ON YOUR SIDE

ESET Deutschland GmbH | Spitzweidenweg 32 | 07743 Jena | Tel.:+49 3641 3114 200

ESET.DE | ESET.AT | ESET.CH