CYBERSECURITY
EXPERTS ON YOUR SIDE

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 alle in ausreichender Qualität von außen 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 und Anwendersoftware, sowie Content 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 Handlungsempfehlungen 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.

CYBERSECURITY EXPERTS ON YOUR SIDE

Home-Office – sicherer Zugriff auf das Firmennetzwerk

In der Corona-Krise arbeiten derzeit viele Mitarbeiter den eigenen vier Wänden. Gerade 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.

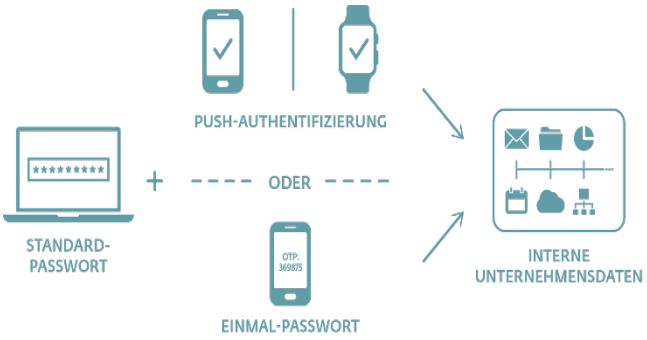
2- oder Multifaktor Authentifizierungen

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.

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 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 sollten 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/pressemitteilungen/pressemitteilungen/eset-startet-hilfsaktion-fuer-unternehmen-zur-absicherung-von-home-offices/

CYBERSECURITY EXPERTS ON YOUR SIDE

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 kriminell-verschlüsselten 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. Erklärungen 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

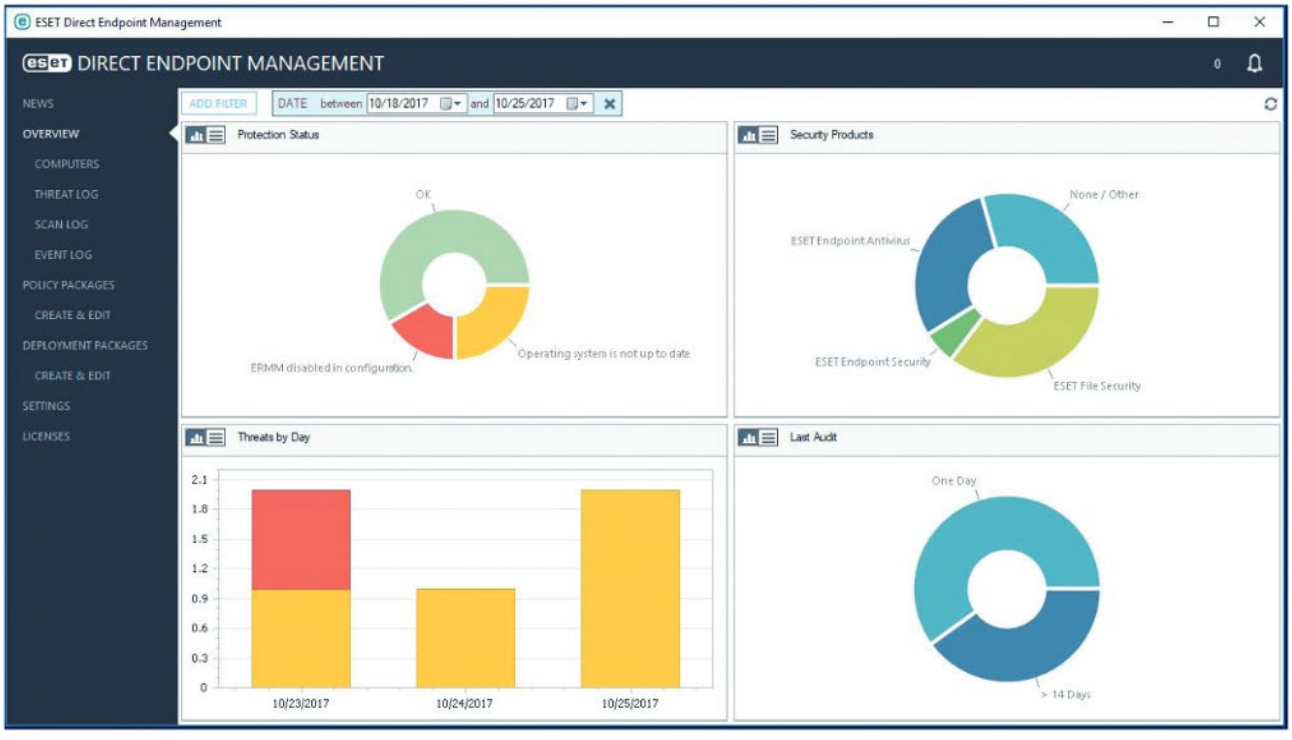
Dieses Thema betrifft vorrangig Ihr IT-Team und/oder Ihren IT-Dienstleister. Gerade in der aktuellen Situation sollten Sie einen ständigen Überblick über die unten aufgeführten Punkte haben. Da dies recht viel werden kann, setzen Sie auf Lösungen, wie etwa beim Thema IT-Security, die Ihnen für viele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



CYBERSECURITY
EXPERTS ON YOUR SIDE

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