Sicher arbeiten
Zu Hause und unterwegs

Quelldokument:	Document1
Version:	v1.0
Auslieferungsdatum:	27. März 2020
Autor:	Jan-Tilo Kirchhoff, Compass Security Deutschland GmbH
Klassifikation:	PUBLIC

Compass Security Deutschland GmbH, Tauentzienstraße 18, 10789 Berlin
T +49 30 21 00 253-0, team.csde@compass-security.com, www.compass-security.com

5 Punkte für die Sicherheit mobiler Arbeitsplätze

Durch die aktuellen Entwicklungen rund um Corona/COVID-19 sehen sich immer mehr Unternehmen gezwungen, ihren Mitarbeitenden die Möglichkeit einzuräumen von zu Hause aus zu arbeiten. Neben sozialen, praktischen und rechtlichen Aspekten hat die Ausübung der beruflichen Tätigkeit weit ab vom gewohnten Arbeitsplatz auch Auswirkungen auf die IT-Sicherheit. Compass Security möchte Ihnen mit diesem Dokument 5 Punkte an die Hand geben, die Sie bei der Einführung mobiler Arbeit berücksichtigen sollten; besonders wenn dies kurzfristig umgesetzt werden soll oder in den letzten Tagen bereits umgesetzt wurde.

1 Der Mensch steht im Mittelpunkt

Gut über IT-Sicherheit informierte Mitarbeitende sind ein wesentlicher Faktor für den Schutz des Unternehmensnetzwerks. Sie können helfen, Angriffe frühzeitig zu erkennen und abzuwehren. Der fehlende direkte Kontakt zu Kollegen, der mit der Arbeit außerhalb des Büros einhergeht, kann die Schutzwirkung jedoch mindern.

Cyberkriminelle nutzen die aktuelle Situation auf unterschiedliche Arten aus. So warnt das BSI beispielsweise vor gefälschten E-Mails der Sparkassen[i] mit denen Betrüger persönliche Daten der Opfer sammeln wollen. Weiterhin sei Vorsicht bei Einladungen zu Video-Konferenzen geboten, die nicht selten zum Installieren einer für die Teilnahme notwendige Software auffordern. Diese kann bei einem Angriff Schadcode enthalten, der den Computer des Mitarbeitenden infiziert und dem Angreifer somit ein Einfallstor in das Unternehmen liefert.

Darüber hinaus gibt es (mobile) Applikationen, die vorgeblich Informationen über Ausbreitung von COVID-19 bereitstellen, tatsächlich aber Daten über die Anwender sammeln[ii].

Auch CEO Fraud, also das Auffordern zur Überweisung von Geldern durch Vorgesetzte per E-Mail oder Telefon, bei dem Mitarbeitende teilweise massiv unter Druck gesetzt werden, ist in der aktuellen Situation eine besondere Bedrohung, da eine persönliche Nachfrage bei Kollegen oder dem Vorgesetzten nicht so leicht möglich ist.

Schaffen Sie eine zentrale Anlaufstelle im Unternehmen, bei der sich Mitarbeitende melden können, wenn ihnen eine E-Mail oder ein Anrufer verdächtig vorkommen. Sorgen Sie dafür, dass die dort eingehenden Informationen bewertet und bei Bedarf alle Mitarbeitenden über neue Angriffsmuster informiert werden.

2 Sicherer Zugang zum Netz

Um die Unternehmensprozesse aufrechtzuerhalten und die Kommunikation untereinander aber auch mit Kunden zu ermöglichen, benötigen die Mitarbeitenden Zugang zum Internet und Unternehmensnetzwerk. Viele datenschutzrechtlich relevanten Aspekte lassen sich diesbezüglich durch organisatorische Maßnahmen regeln. Die technische Sicherheit sollte aber bei aller gebotenen Eile ebenfalls nicht vernachlässigt werden.

Leider ist zu beobachten, dass in den letzten Tagen und Wochen vermehrt E-Mail- und Applikationsserver, die bisher für den internen Einsatz konfiguriert waren, nun im Internet erreichbar gemacht wurden. Hierdurch vergrößert sich die Angriffsfläche eines Unternehmens enorm, da gerade intern genutzte Systeme oft nicht hinreichend sicher konfiguriert und mit den notwendigen Sicherheitsupdates versorgt werden. Grundsätzlich ist zu empfehlen, den Zugang zu Unternehmensressourcen über virtuelle private Netze (VPN) abzusichern. Sollte dies aus dem einen oder anderen Grund nicht möglich sein, sollten die Systeme zumindest wie in den folgenden zwei Punkten beschrieben mit der aktuellsten Software ausgestattet und die Zugriffskontrolle verschärft werden.

Auch die Zugangsnetze, also der öffentliche Hotspot oder das heimische Netzwerk bieten mögliche Angriffspunkte. Ggf. werden diese von Partnern, Kindern und manchmal auch von Nachbarn mitgenutzt. Daher sollten alle Daten verschlüsselt, am besten durch das Unternehmens-VPN übertragen werden.

Wird das VPN so konfiguriert, dass lediglich die Zugriffe auf das Unternehmensnetz geschützt werden, der Zugang zum Internet aber direkt erfolgt, scheint dies im Sinne einer Bandbreitenoptimierung vielleicht sinnvoll. Den Angreifern bzw. deren Malware öffnet es jedoch einen direkten Zugriff auf mit dem Unternehmensnetz verbundene Systeme, da eine nicht durch die Unternehmensfirewall überwachte Kommunikation über Internet möglich ist.

Auch der Schutz der lokalen Systeme ist wichtig. So sollte der Zugang zum heimische WLAN mit einem starken Kennwort und WPA2 Verschlüsselung geschützt und der administrative Zugriff auf den Router mit einem komplexen Passwort gesichert werden.

3 Passwörter, etc.

Über die Sicherheit von Passwörtern wurde schon viel geschrieben. Den Empfehlungen des BSI zu diesem Thema[iii] ist kaum etwas hinzuzufügen.

In der aktuellen Situation sollte jedoch besonders darauf geachtet werden, insbesondere wenn bisher nur intern erreichbare Systeme und Applikationen nun direkt vom Internet aus zu erreichen sind. Aus unseren Penetrationstests wissen wir, dass gerade bei internen Webanwendungen häufig simple Passwörter verwendet werden und somit kein hinreichender Schutz vor Brute-Force Attacken gegeben ist; häufig mit der Begründung, dass ein Angreifer zunächst Zugang zum internen Netz erlangen müsste und das Schutzniveau ausreichend sei.

Um den Umgang mit einer Vielzahl von komplexen Passwörtern zu erleichtern ist der Einsatz eines Passwortmanagers zu empfehlen. Weiterhin sollten besonders kritische Systeme wie VPN-Zugänge oder Web-Mail durch zertifikatsbasierte Authentisierung und/oder Multifaktor Authentisierung zusätzlich geschützt werden.

4 Sind Sie auf dem aktuellen Stand?

Auch das oft stiefmütterlich behandelte Patch Management gewinnt in der aktuellen Situation an zusätzlicher Bedeutung. Computer, die bisher im internen Netzwerk des Unternehmens genutzt wurden, werden den Mitarbeitenden nun für die Arbeit zu Hause zur Verfügung gestellt und haben damit unter Umständen keinen Zugriff mehr auf zentrale Update Server des Unternehmens.

Teilweise stehen nicht genügend transportable Computer zur Verfügung und Mitarbeitende nutzen den privaten Rechner. Abgesehen von den datenschutzrechtlichen Unwägbarkeiten ist das Unternehmen nicht in der Lage hier aktiv für einen aktuellen und sicheren Stand des Betriebssystems und der eingesetzten Software zu sorgen. Diese Situation sollte soweit möglich vermieden werden. Eine Alternative kann die Bereitstellung von virtuellen Maschinen für die Mitarbeitenden sein, die dann wieder vollständig vom Unternehmen kontrolliert werden können. Mindestens sollten die Mitarbeitenden angewiesen werden nur aktuelle und lizensierte Software einzusetzen. Dies gilt auch für heimische Infrastruktur, wie z.B. Router oder Drucker.

5 Arbeitsmittel sind kein Spielzeug

Durch die Vermischung von Arbeit und häuslichem Umfeld haben Familienmitglieder, insbesondere auch Kinder physischen Zugang zu Firmen-Laptops, Tablets, etc. Noch mehr als im Büro sollte beim Verlassen des Rechners der Desktop gesperrt werden, um unerwünschte Zugriffe zu verhindern, sonst sind schnell durch einen unbedachten Mausklick die Ergebnisse eines halben Arbeitstages vernichtet oder ein wichtiger Auftrag storniert.

In der aktuellen Lage kommt natürlich auch Langeweile auf; warum also nicht mal schnell ein Spiel auf dem Firmenhandy installieren, damit der Nachwuchs ruhiggestellt ist und man in Ruhe weiterarbeiten kann? Auch hier ist zu bedenken, dass ggf. Zugriff auf alle auf dem Gerät installierten Applikationen besteht oder im schlimmsten Falle das kostenlose Spiel noch einige zusätzliche Schadfunktionen mitliefert.

Schließlich müssen Laptop oder PC auch vom Büro nach Hause und in hoffentlich nicht allzu ferner Zukunft wieder zurück transportiert werden. Damit beim Transport keine Daten in falsche Hände geraten, sollten die Festplatten der Systeme generell verschlüsselt werden. Wenn dann doch mal ein Rechner vom Beifahrersitz entwendet wird, ist zumindest der Datenschutz gewährleistet.

Fazit

Unternehmen und Vorgesetzte sind gut beraten ihren Mitarbeitenden entsprechende Hinweise und Anweisungen für den Umgang mit der (Unternehmens-) IT zu Hause und unterwegs an die Hand zu geben und die technischen Voraussetzungen für sicheres Arbeit in jeder Lage zu schaffen.

Wenn Sie Fragen zum Thema haben unterstützt Compass Security Sie gerne, sei es bei der Überprüfung der technischen Schutzmaßnahmen oder durch Webinare für Sie und Ihre Mitarbeitenden.

Compass Security Deutschland GmbH
team.csde@compass-security.com
Tel.: +49 30 2100 253 0

[i] https://www.bsi-fuer-buerger.de/BSIFB/DE/Service/Aktuell/Informationen/Artikel/corona-falschmeldungen.html
[ii] https://blog.lookout.com/commercial-surveillanceware-operators-latest-to-take-advantage-of-covid-19

[iii] https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/bausteine/ORP/ORP_4_Identit%C3%A4ts-_und_Berechtigungsmanagement.html?nn=10137172#doc10095784bodyText9