Thema: Informationssicherheit

In diesen Wochen arbeiten so viele Menschen von zu Hause, wie wohl noch nie zuvor in der Geschichte. Für manche Mitarbeiter ist es Gewohnheit, weil ihre Arbeitgeber das schon lange erlauben. Für andere hingegen ist es das erste Mal. Und es sitzen nicht nur Erwachsene an den Esstischen und Küchenarbeitsplatten der Republik, sondern auch die Kinder, deren Schulen geschlossen sind. Es ist eben eine Ausnahmesituation. Genau das wissen auch Cyberkriminelle und so sind Anstiege der Cyber-Angriffe zu verzeichnen.

Keiner der Angriffsmechanismen ist dabei wirklich neu. Allerdings treffen die Angriffe auf veränderte Rahmenbedingungen, weil zum Einen die Isolation für veränderte Kommunikationswege zwischen den Kollegen sorgt und zum Anderen die Internetzugänge zu Hause oft weniger professionell abgesichert sind.

Hier die wichtigsten **Tipps für Sie als Mitarbeiter**:

Superkurzform für Eilige: Seien Sie wachsam und misstrauisch, klicken Sie keine Links an, öffnen Sie keine Anhänge, nutzen Sie nur die dienstlich gestellte Hardware, melden Sie Vorfälle sofort!

Jetzt ein wenig ausführlicher. Die wichtigste Regel gegen Cybercrime ist und bleibt: **Seien Sie wachsam!** Ja, Harry Potter Fans dürfen sich hier gerne Mad-Eye Moody vorstellen. Denken Sie daran, dass Panikmache ein Geschäftsmodell ist und dass Cyberkriminelle schon immer auf aktuelle Entwicklungen aufgesprungen sind, um Sie dazu zu bewegen, doch einen kurzen Moment lang unachtsam zu sein. Das ist nichts Neues, durch das Coronavirus Ausgelöstes, sondern deren übliches Geschäftsmodell.

Wichtige Informationen zur Pandemie erhalten Sie NICHT unaufgefordert per Mail! Sollten also E-Mails bei Ihnen ankommen, die Pandemieinformationen versprechen, seien Sie grundsätzlich misstrauisch. Klicken Sie nicht auf darin befindliche Links und öffnen Sie keine Anhänge.
In solchen Mails haben sich die kriminellen Absender in den letzten Tagen z. B. als Mitarbeiter der Weltgesundheitsorganisation, als Universitätsmitarbeiter oder auch als IT-Techniker ausgegeben.

Es gab Falschmeldungen, dass in bestimmten Städten die Krankenhäuser voll belegt seien und Sie daher unbedingt sofort Atemschutzmasken kaufen sollten, um sich zu schützen. Der vermeintliche Webshop, der sich dahinter verbarg, war gefälscht und das per Kreditkarte gezahlte Geld verloren. Auch hier gilt: Seien Sie misstrauisch! Egal, ob man Ihnen Atemschutzmasken, Wasserfilter oder andere angeblich dringend notwendige Dinge zum Kauf anbietet. Oft steckt dahinter ein Betrug, um an Ihre Kreditkartendaten zu kommen oder Ihnen Schadsoftware unterzujubeln. Es wird auch versucht, Sie mit angeblichen begrenzten Mengen zeitlich unter Druck zu setzen. Bleiben Sie ruhig und besonnen.

Wenn Sie doch einen Link angeklickt haben, kann es sein, dass man Sie auf täuschend echte Anmeldemasken weiterleitet, die z. B. aussehen wie bei OneDrive bzw. Office 365. Seien Sie auch hier extrem misstrauisch und geben Sie beim leisesten Zweifel keine Anmeldeinformationen ein.

Auf Android Smartphones wird für eine App geworben, die angeblich live den Verlauf der Virusausbreitung anzeigen kann. Die Wahrheit dahinter? Wenn Sie die App installieren, wird Ihr Smartphone verschlüsselt, sodass Sie nicht mehr an Ihre Daten rankommen und Sie werden zur Zahlung von Lösegeld aufgefordert.

Melden Sie Vorfälle, die cyberkriminell sind oder sein könnten, **unverzüglich** in Ihrem Unternehmen. Sollte z. B. Ihr dienstlicher Laptop von einem Virus betroffen sein, könnte dieser sich im Firmennetzwerk ausbreiten, auch wenn Sie von zu Hause arbeiten. Daher ist Ihre schnelle Meldung wichtig, um einen Schaden möglichst rasch einzudämmen.

Nutzen Sie die Hardware, die Sie vom Unternehmen bekommen haben. Wenn wir davon ausgehen, dass Sie als Leser kein IT-Spezialist sind, ist die dienstliche Hardware vermutlich besser abgesichert als Ihr privater Computer. Zudem wird Ihr Arbeitgeber eh darauf bestehen, dass Sie mit Unternehmensdaten nur auf unternehmenseigenen Systemen arbeiten dürfen. Und das gilt übrigens gleichermaßen für Smartphones. Halten Sie sich auch an die Vorgaben des Unternehmens. Bevor Sie mit Ihren Kollegen aus der vermeintlichen Not heraus WhatsApp Gruppen bilden und darüber dienstliche Dinge regeln, klären Sie unbedingt, ob das erlaubt ist. Unser Tipp: Lassen Sie es bleiben.

Wo bekommen Sie seriöse Infos zur Pandemie? Zum Beispiel hier:

- https://www.bundesregierung.de/breg-de/themen/coronavirus/coronavirus-1725960
- https://www.bundesgesundheitsministerium.de/coronavirus.html
- https://www.who.int/emergencies/diseases/novel-coronavirus-2019
- https://www.rki.de/DE/Content/InfAZ/N/Neuartiges_Coronavirus/Fallzahlen.html

Hier die wichtigsten **Tipps für Sie als Unternehmen**:

Denken Sie daran, dass die Heimnetzwerke Ihrer Mitarbeiter oft nicht so gut abgesichert sind, wie Ihre Firmennetzwerke. Sorgen Sie daher dafür, dass die Hardware im Homeoffice gut geschützt ist: Verschlüsseln Sie die Laptops und Smartphones Ihrer Mitarbeiter. Wenn möglich, richten Sie Mechanismen ein, um Mobilgeräte auch aus der Ferne sperren und löschen zu können.

Der Zugang zu Ihrem Netzwerk sollte natürlich gut abgesichert sein. VPN und wenn möglich Zwei-Faktor-Authentifizierung sind da z. B. Mittel der Wahl. Vermutlich hat Ihre IT-Abteilung in den letzten zwei Wochen enorme Arbeitsmengen bewältigen müssen, um eine viel höhere Anzahl Mitarbeiter als gewohnt ins Homeoffice bringen zu können. Vertrauen Sie Ihren Spezialisten und den Lösungen, die sie Ihnen vorschlagen. Das gilt sowohl für Software als auch für Hardware: Ein Tool mag ein paar Euro teurer sein, die aber gut angelegt sind, wenn es deutlich weniger aufwändig zu verwalten ist. Und ja, es kommt schon zu Engpässen bei Hardware. Wir selbst haben Ende letzter Woche Preisanstiege von 100 % und mehr bei Webcams beobachtet. Das sagen die IT-Kollegen nicht, um teurere „Spielzeuge" kaufen zu dürfen.

Vermutlich wollen Sie Tools zur Zusammenarbeit im Homeoffice einsetzen. Wir werden dem Thema noch einen eigenen Newsletter widmen, aber bitte bedenken Sie schon jetzt: Steuern Sie diese Tools frühzeitig. Stellen Sie den Mitarbeitern Chats, Videokonferenzsysteme und Möglichkeiten zum Teilen von Dokumenten zur Verfügung. Denken Sie auch daran, Ihnen Anleitungen für den Umgang mit diesen Tools zu geben. Für viele ist die Arbeit von zu Hause ungewohnt und neu, und Neues macht unsicher. Eines ist aber sicher: Wenn Sie nichts „liefern", werden die Menschen sich Lösungen (wie nicht von Ihnen genehmigte Chatgruppen auf Smartphones) suchen. Und solche Schatten-IT-Konstrukte einzufangen, wird dann eine schwierige Aufgabe – und ein Informationssicherheitsvorfall – sein.

Ein letzter Punkt: Es sind nicht nur die Mitarbeiter selbst im Homeoffice. Auch die Kinder Ihrer Mitarbeiter oder die Großeltern verbringen plötzlich mehr Zeit als vorher an den heimischen Computern und Tablets. Seien Sie fürsorglich und ermutigen Sie Ihre Mitarbeiter, die Tipps gegen Cyberkriminalität auch mit der Familie zu teilen.

Quellen zu Cyberangriffen und gute Tipps für Ihre Mitarbeiter derzeit:

- https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/coronavirus-used-in-spam-malware-file-names-and-malicious-domains
- https://www.ncsc.gov.uk/guidance/home-working
- https://www.bmi.gv.at/news.aspx?id=7745347A7971512F6968343D

Sie brauchen **kurzfristig und kostenfrei einen Expertenrat** zum Thema
Business Continuity / Krisen- und Notfallmanagement,
dann schreiben Sie uns oder rufen Sie uns an!

RUCON Service GmbH, Neumeyerstraße 48, 90411 Nürnberg
Telefon: +49 911 / 47 75 28-0 - E-Mail: mail@msaas.com

www.rucon-group.com Das Buch www.msaas.com Newsletter

#surviveANDprosper #surviveANDprosper #surviveANDprosper #surviveANDprosper #surviveANDprosper