Cyberrisiken in Zeiten des Coronavirus

März 2020

Beobachtungen

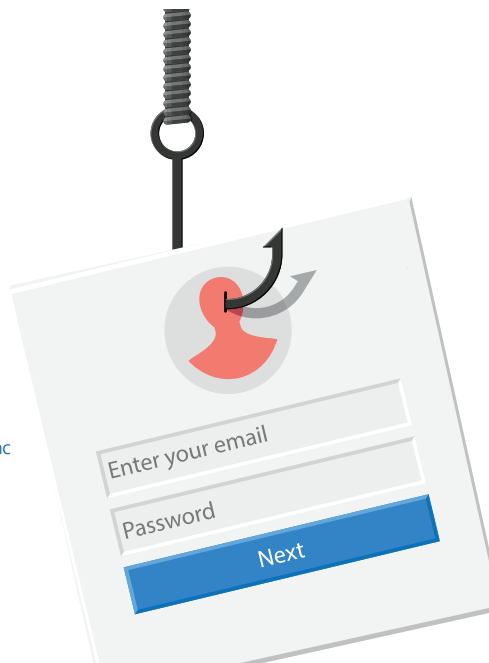
In den letzten Wochen verzeichneten Unternehmen weltweit einen drastischen Anstieg der Zahl der Cybervorfälle. Diese werden durch eine neue Welle von Cyberangriffen unter dem Deckmantel des Themas Coronavirus ausgelöst. Laut dem Unternehmen für Cybersicherheit CYE nutzen Cyberkriminelle die unsichere Lage angesichts der globalen Pandemie seit Anfang Februar zunehmend aus. CYE hat eine fünfmal höhere Zahl an Vorfällen verzeichnet, besonders in Europa.

Aufgrund der allgemeinen Angst und zunehmenden Verwirrung im Zusammenhang mit den aktuellen Ereignissen steigt die Wahrscheinlichkeit, dass Mitarbeitende schädliche Anhänge anklicken oder über unsichere Netzwerke von zu Hause oder von anderen Standorten aus auf sensible Daten zugreifen. Es wird immer wichtiger, abteilungsübergreifend verstärkt auf angemessene Kontrollen zu achten – zumal immer häufiger Quarantänen verhängt werden und immer mehr Mitarbeitende per Fernzugriff arbeiten.

Jüngsten Studien zufolge ist die Zahl der Phishing-Kampagnen und Ransomware-Angriffe in den letzten Wochen besonders gestiegen: Oft haben Nutzer Anhänge oder Links angeklickt, die das Coronavirus-Thema nutzen, um schädliche Nachrichten zu verbreiten.

Bei einem raffinierten Angriff wurde sogar die vertrauenswürdige Stellung der Weltgesundheitsorganisation (WHO) ausgenutzt: Fälschlicherweise wurde behauptet, dass Mitarbeitende der WHO sensible Daten erfragen würden. Stattdessen wurde ein Anhang verbreitet, über den personenbezogene Daten gestohlen wurden.

Abbildung 1: Screenshot einer Phishing-E-Mail, die angeblich von der Weltgesundheitsorganisation stammen sollte – Quelle: Proofpoint inc



[1] https://blog.checkpoint.com/2020/03/05/update-coronavirus-themed-domains-50-more-likely-to-be-malicious-than-other-domains/amp/

Erhöhte Cyberrisiken

Wer per Fernzugriff und dezentralisiert arbeitet, hat ein höheres Risiko, den folgenden Angriffsarten zum Opfer zu fallen:

Phishing/Spear Phishing: Das sind E-Mails oder andere elektronische Mitteilungen, die konkrete Daten des Empfängers enthalten. So soll der Leser dazu verleitet werden, einen Link anzuklicken, einen schädlichen Anhang zu öffnen oder andere gefährliche Handlungen durchzuführen.

Business Email Compromise (BEC): Betrugsschema per E-Mail, bei dem die Empfänger dazu gebracht werden sollen, Überweisungen zu veranlassen. Meistens gibt sich der Absender als CEO, CFO oder eine andere Führungskraft des Unternehmens aus.

Social Engineering: Psychologische Manipulation von Menschen, so dass sie Dinge tun, die sie normalerweise nicht tun würden.

Diese Vorfälle bergen ein erhöhtes Risiko der Ausbreitung von Ransomware, die nicht nur die Computernetzwerke von Unternehmen und ihren Kunden infizieren und sperren, sondern auch Daten verschlüsseln oder zerstören kann. Wenn man bedenkt, dass einige Formen von Cyberangriffen tage-, monate- oder gar jahrelang schlummern können, dann könnten sich Handlungen von heute noch weit in der Zukunft massgeblich auf die Erträge und den Ruf eines Unternehmens auswirken. Glücklicherweise haben Unternehmen und Mitarbeitende verschiedene Möglichkeiten, um solche Handlungen durch vorbeugende Massnahmen zu vermeiden und ein sicheres, geschütztes digitales Umfeld zu wahren.

Empfehlungen zur Risikobegrenzung

Einzelpersonen:

Links/Anhänge: Klicken Sie keine Links oder Anhänge in E-Mails an, wenn der Absender nicht vertrauenswürdig ist. Wenn Sie im Internet eine Seite aufrufen möchten, dann geben Sie die URL der Seite, die Sie besuchen möchten, am besten direkt ein. Eine sichere URL beginnt mit https anstelle von http, aber dieses Kriterium reicht noch nicht aus: Schauen Sie sich die URL genau an, bevor Sie sie eingeben, um sicherzugehen, dass sie zu der offiziellen Website des Unternehmens/der Einrichtung führt, die Sie aufrufen möchten. Nutzen Sie bei Zweifeln vor dem Aufruf einen Online-Prüfdienst für URLs, zum Beispiel **isitphishing.org**.

Daten: Antworten Sie keinen unbekannten Quellen und geben Sie ihnen keine Kontodaten preis. Vertrauenswürdige Unternehmen wie Lieferanten oder Vertragspartner verfügen in der Regel bereits über diese Daten. Übermitteln Sie unbekannten Personen niemals Kennwörter oder Daten, mit denen Ihre Identität ermittelt werden könnte, und öffnen Sie keine Anhänge in E-Mails, die Sie nicht angefordert haben.

Melden Sie verdächtige Vorgänge: Alle verdächtigen E-Mails sollten dem Team für Cybersicherheit oder einer vergleichbaren Abteilung des Unternehmens gemeldet werden.

Benachrichtigen Sie den Help Desk: Alle Mitarbeitenden sollten ihren Help Desk vor Ort informieren, wenn sie glauben, dass sie einen Anhang geöffnet oder einen Link angeklickt haben, durch den ihr Computer mit Schadsoftware infiziert wurde.

Abschliessende Gedanken und Überlegungen

Es liegt in der Natur des Menschen, dass wir uns auf das konzentrieren, was wir sehen. COVID-19 erinnert uns daran, dass unsichtbare und nicht greifbare Risiken mitunter viel schlimmer sein können als die konkreteren Risiken, die wir jeden Tag sehen oder von denen wir lesen. Genau wie COVID-19 fallen auch Cyberangriffe in diese Kategorie der nicht greifbaren Risiken. In den letzten Jahren haben wir mehrmals erlebt, wie digitale Viren Maschine um Maschine infiziert und sich in kürzester Zeit zu einer wahren Pandemie ausgebreitet haben. Die bisher grösste Pandemie dieser Art war der NotPetya-Vorfall im Jahr 2017. Damals waren tausende Unternehmen rund um den Globus betroffen, was Schätzungen zufolge zu einem wirtschaftlichen Schaden von zehn Milliarden US-Dollar führte. Hygiene ist unerlässlich, um eine Infektion von vornherein zu vermeiden. Das gilt für die Gesundheit genauso wie für IT-Sicherheit: Patches und Händewaschen lassen sich in ihrer Bedeutung vergleichen. Bei der Eindämmung möglicher Ansteckungen weisen Sandboxing und Quarantänen erstaunliche Ähnlichkeiten auf.

Im Cyberbereich bietet das US-amerikanische National Institute of Standards and Technology (NIST) einen Referenzrahmen für Unternehmen zum Ausbau ihrer Ressourcen: Sie können so Cyberrisiken erkennen und sich vor Cyberangriffen schützen, sie feststellen, darauf reagieren und die Systeme wiederherstellen. Diese Ressourcen umfassen Technologie, beschränken sich aber nicht nur darauf. Wie eingangs erwähnt, beruht der Schutz vor allem auf Verfahren und dem Bewusstsein der Mitarbeitenden. Entscheidend ist, dass Vorfälle zuverlässig und schnell festgestellt werden und dass bei Bedarf angemessen reagiert wird, um die Systeme wiederherzustellen. Darüber hinaus liefert uns die aktuelle Situation rund um COVID-19 folgende Erkenntnisse: Wie gehen wir mit plötzlichen Nachfrageschüben nach Schutzmechanismen um? Handdesinfektionsmittel und Schutzmasken sind selten geworden, und medizinische Fachkräfte kommen bei den steigenden Patientenzahlen auf den Intensivstationen kaum hinterher.

Vor diesem Hintergrund sollten wir uns fragen, wie sich das auf den Cyberbereich und die nächste Cyberpandemie übertragen lässt: Können wir uns auf unseren Cyberschutz verlassen und auf unsere Ressourcen und Fähigkeiten, darauf zu reagieren? Können wir uns im Falle einer Cyberpandemie auf unsere externen Dienstleister verlassen, wenn wir bedenken, dass sie unzählige Kunden haben und ihre knappen Ressourcen dann nach Prioritäten aufteilen müssen?

Unternehmen:

Schulung von Mitarbeitenden/Nutzern zur Bewusstseinsbildung: Bevor ein Unternehmen Fernzugriffe auf das Firmennetzwerk zulässt, sollten die Mitarbeitenden eine angemessene Schulung zu Phishing-Kampagnen und Sicherheitsrichtlinien erhalten. Ausserdem sollten sie alle Prozesse und Verfahren des Unternehmens zur Meldung eines Sicherheitsvorfalls kennen – für den Fall, dass ein Angriff vermutet oder entdeckt wird.

Sichere Verbindungen: Nutzen Sie Firmennetzwerke ausschliesslich über einen sicheren Fernzugang. Das sollte nach Möglichkeit ein virtuelles privates Netzwerk (VPN) oder ein anderes verschlüsseltes Verbindungsverfahren sein.

Multifaktorauthentifizierung (MFA): Als zusätzliche Sicherheit sollten VPNs mit einer Multifaktorauthentifizierung konfiguriert sein, damit wirklich nur befugte Personen auf das Firmennetzwerk zugreifen.

Mobilgeräteverwaltung (MDM): Computer, Tablets und Smartphones der Mitarbeitenden sollten mit einer MDM-Lösung des Unternehmens ausgestattet sein. Die Lösung sollte angemessene Sicherheitskontrollen gewährleisten und im Gerät ein verschlüsseltes virtuelles Umfeld schaffen, in dem Firmendaten wie Dokumente und E-Mails gespeichert und bearbeitet werden können.

Internet-Umgebungsschutz: IT-Abteilungen sollten dafür sorgen, dass Firewalls richtig konfiguriert sind, und die Protokollierung der Firewall überwachen, damit sich Verbindungsversuche oder ein erfolgreicher Verbindungsaufbau von unbefugten oder verdächtigen Internet-Protokoll-Adressen (IP-Adressen) nachvollziehen lassen.

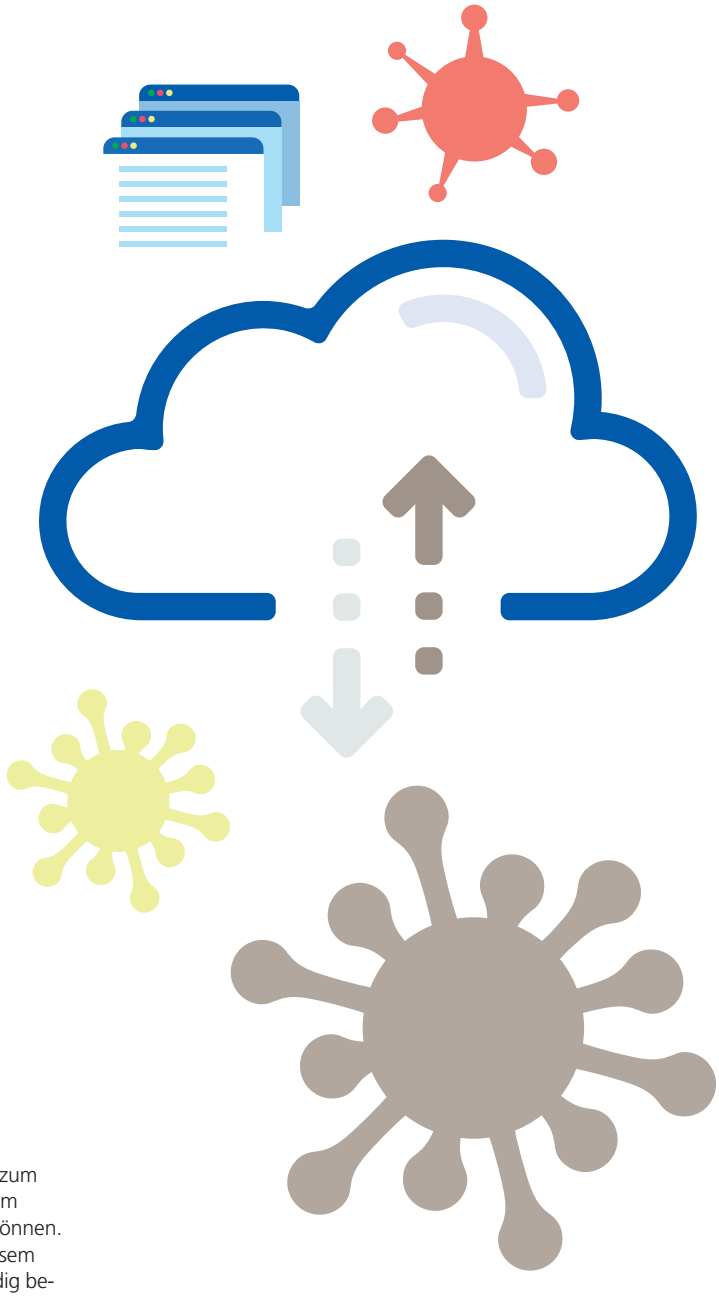
Cloud-Sicherheit und Einhaltung von Vorschriften: Unternehmen, die Cloud-Dienste nutzen, sollten darauf achten, dass die Sicherheitseinstellungen in angemessener Weise verschärft und auf Konfigurationsveränderungen oder unbefugte Manipulation geprüft werden.

Erhöhte Kontrolle und Sorgfalt: Gibt es Regionen oder Länder, in denen kein Grund für einen Fernzugriff durch Mitarbeitende über das Firmennetzwerk besteht? Dann sollte die IT-Abteilung die IP-Bereiche dieser Regionen aktiv auf die «schwarze Liste» setzen, um einen Fernzugang von dort zu den Firmennetzwerken zu verhindern.

Sind unsere internen Ressourcen für die Cybersicherheit des Unternehmens und für Reaktionen im Notfall autark?

Schliesslich hat uns COVID-19 aufgezeigt, wie komplex sich unsere Lieferketten gestalten und wie abhängig wir von Zwischenerzeugnissen aus anderen Ländern und von anderen Kontinenten sind. Heutzutage gilt dies nicht nur für Lieferanten physischer Waren, sondern auch für die Anbieter von Rechenleistung, Datenspeicherung und Plattformen, auf denen Apps laufen.

Ein grosser Trend im verarbeitenden Gewerbe bestand in den letzten Jahrzehnten in der Auslagerung von Prozessen, gefolgt von der Verlagerung von Dienstleistungen ins Ausland. Gleiches war in der Informationstechnologie zu beobachten. Heute ist der Einsatz der Cloud der nächste Schritt, und viele Unternehmen migrieren ihre IT-Infrastrukturen zurzeit in die Clouds grosser Dienstleister. Die deutlich (kosten-) effizientere Arbeitsweise, die dank cloudbasierter Lösungen technisch möglich wird, trägt dazu bei, dass wir besser auf eine Pandemie in der realen Welt reagieren und uns von ihr erholen können. Zugleich entsteht so die nächste nicht greifbare, unsichtbare Schwachstelle. Während wir noch nach dem «Notausschalter» für COVID-19 suchen, können wir bereits überlegen, was das Virus uns über unsere digitale Belastbarkeit und Cybersicherheit sagt und an welchen Stellen wir uns auf die nächste Cybervirus-Epidemie vorbereiten müssen.



ZH27859d-2003

ZURICH®