Cyber-Risiken in Zeiten des Corona-Virus

Einführung

Seitdem das Corona-Virus rund um den Globus für Schlagzeilen sorgt, verzeichnen Firmen weltweit einen signifikanten Anstieg von Cybervorfällen. Diese Vorfälle werden unter dem Vorwand von Corona ausgelöst. Die aktuelle Lage der globalen Pandemie wird damit ungeniert ausgenutzt.

Die allgemeine Angst und Verunsicherung sowie die Home Office Tätigkeiten erhöhen das Risiko, dass Angestellte schädliche Dateien anklicken oder von unsicheren Netzwerken aus auf sensible Daten zugreifen. Aktuelle Studien zeigen eine erhebliche Anzahl von neuen Phishing-Kampagnen und Ransomeware-Angriffen.

Gerne wollen wir Ihnen in diesem Artikel entsprechende Tipps und Empfehlungen, basierend auf der Expertise von Neo One, unserem Partner für IT und Cyber Security Fragen, geben.

Es ist uns ein grosses Bedürfnis, Sie in dieser schwierigen Phase zu unterstützen und auf das erhöhte Cyber Risiko aufmerksam zu machen. Gerne stehen wir Ihnen wie bis anhin auch für alle Fragen rund um eine Cyber-Risk Versicherung zur Verfügung.

Die Gefahren von Covid-19

Sowohl die Wirtschaft als auch Privatpersonen erleben aktuell eine Zeit, in welcher Sicherheit in vielen Aspekten grossgeschrieben wird. Leider werden die Gefahren in Bezug auf Cyber-Risiken jedoch nach wie vor stark unterschätzt. Die Zunahme von Cyber-Attacken häufen sich im Bereich von gefälschten E-Mails zu den Themen Corona Virus, SARS-CoV-2, Covid-19 und ähnlichen Verlautbarungen. Damit versuchen Cyberkriminelle unter Ausnutzung der aktuellen Situation, Schadsoftware zu verbreiten und Geräte damit zu infizieren. Als Absender werden u.a. das Bundesamt für Gesundheit, die Weltgesundheitsorganisation oder irgendwelche Forschungsinstitute angegeben, was den «Fake» noch realer erscheinen lässt.

Die Wirtschaft hat in den letzten Wochen in einem nie vorher dagewesenen Ausmass auf Home Office Arbeit umgestellt. Diese Situation wird von Betrügern ausgenutzt, um zum Beispiel mittels gefälschten E-Mails dringende Zahlungen auszulösen oder auch um Zugriffe auf die Unternehmenssysteme via Home Office Zugängen zu erwirken.

Angriffsmeldungen, Verschlüsselungen von Daten, Datenverluste und Lösegeld-Forderungen führen oftmals zum Stillstand von Unternehmen. Viele Unternehmen stellen dann fest, dass Sie über kein funktionierendes Backup, über ungenügende Notfallszenarien und Schutzmassnahmen verfügen.

Das Corona-Virus bzw. die entsprechende Pandemie haben einen massiven Einfluss auf die IT und die Arbeitsweise der Mitarbeitenden. Das Unwort 2020 ist mit Sicherheit schon vergeben und heisst Corona. Das am meisten gebrauchte Wort im 2020 ist jedoch ein anderes: «Home Office». Wenn wir uns die aktuelle Situation anschauen, stellt das Corona-Virus neue Anforderungen an die Informatik in den Betrieben.

Wachsamkeit zählt

Seien Sie in nächster Zeit besonders vorsichtig mit Ihren Zugängen und E-Mails! Mit der zurzeit herrschenden Angst im Zusammenhang mit dem Corona-Virus, steigt die Wahrscheinlichkeit, dass Mitarbeitende schädliche Anhänge anklicken und über unsichere Netzwerke von zu Hause oder anderen Standorten aus auf sensible Daten zugreifen. Angriffe auf Infrastrukturen in allen Unternehmensbranchen und Grössen sind gemäss jüngsten Studien des Bundes allgegenwärtig und in den letzten Wochen besonders gestiegen.

Empfehlungen zur Risikobegrenzung

Nachstehend zeigen wir Ihnen potenzielle Risiken inklusive Tipps zur Risikobegrenzung auf:

Phishing

Mittels gefälschten E-Mails wird versucht an Passwörter oder Kreditkartendaten zu gelangen oder einen Computervirus zu verbreiten.

Eine Phishing-Mail kann ein verlockendes Angebot unterbreiten oder sofortige Handlung Ihrerseits verlangen, um Sie dazu zu bringen ein gefälschtes Formular auszufüllen, den Link zu einer gefälschten Webseite zu klicken oder einen infizierten Anhang zu öffnen.

Tipps

- Zeigen Sie solche E-Mails mittels eines Fotos umgehend einer IT-Fachperson
- Leiten Sie solche E-Mails nicht weiter, sondern löschen Sie sie umgehend ohne Inhalte anzuklicken
- Sollten diese E-Mails nicht in Ihren Spamordner gelangt sein, so gilt es, Ihre Security-Systeme dringend zu optimieren
- Achten Sie auf ganzheitliche Sicherheitskonzepte. Sicherheitskonzepte müssen alle relevanten Unternehmensbereiche umfassen. Sicherheit heisst: Informatiklösungen, Webplattformen und Digitale Systeme aufeinander abzustimmen.

Business E-Mail Compromise

Eine weitere sehr verbreitete und bekannte Masche sind betrügerische Zahlungsanforderungen, welche hauptsächlich an den CEO des Unternehmens geschickt werden. Hierbei werden keine Daten verschlüsselt oder gelöscht, sondern es wird einzig beabsichtigt, Geldtransfers zu

Advantis Versicherungsberatung AG
Buckhauserstrasse 17
8048 Zürich

Neo One AG
Grindelstrasse 6
8303 Bassersdorf

manipulieren. Das Perfide an dieser Zahlungsanforderung ist, dass der Absender in der Regel aus den eigenen Reihen kommt, sprich z.B. von der Finanzabteilung. Die Betrüger ändern die Absendermailadresse so, dass es effektiv so aussieht, als kommt die Anfrage für eine Zahlung von dem bekannten Teamkollegen von nebenan. Erst wenn man das Mail genauer analysiert, z.B. über das Maillog des Spam-Schutzes, kann man erkennen, dass die Absender-Mailadresse gefälscht ist.

Antwortet nun der CEO auf dieses Mail, erfolgen in der Regel Kontoverbindungen und weitere Zahlungsinformationen. Natürlich sollten hier bei solch hohen Beträgen bereits die Alarmglocken klingeln. Diese Beträge können aber auch wesentlich tiefer ausfallen und somit ggf. unbemerkt ausgeführt werden.

Tipps

- Lieber einmal kurz telefonisch nachfragen, wenn man nicht sicher ist oder etwas «komisch» findet
- Zeigen Sie solche E-Mails mittels eines Fotos umgehend einer IT-Fachperson
- Leiten Sie solche E-Mails nicht weiter
- Löschen Sie solche E-Mails umgehend ohne Inhalte anzuklicken
- Sollten diese E-Mails nicht in Ihren Spamordner gelangt sein, so gilt es, Ihre Security-Systeme dringend zu optimieren
- Achten Sie auf ganzheitliche Sicherheitskonzepte. Sicherheitskonzepte müssen alle relevanten Unternehmensbereiche umfassen. Sicherheit heisst: Informatiklösungen, Webplattformen und Digitale Systeme aufeinander abzustimmen.

Cyber-Bedrohung Cloud basiert

Inzwischen stammt fast die Hälfte aller bösartigen Bedrohungen aus der Cloud. Täglich nutzen fast 90 Prozent eine Cloud-App. Dabei werden Cloud-Speicher, Kollaboration- und Webmail-Anwendungen am häufigsten verwendet.

Die Angreifer nutzen die Cloud, um sich unauffällig Zugriff zu verschaffen. Cyberkriminelle starten ihre Attacken häufig über Cloud-Dienste und -Apps und verwenden dabei bekannte Techniken. Die beiden beliebtesten Angriffstechniken aus der Cloud sind Phishing und die Verbreitung von Malware.

Unter anderem gehören Apps wie Microsoft Office 365 for Business, Box, Google Drive, Microsoft Azure, Github und weitere täglich x-fach genutzte Anwendungen zu den meisten angegriffenen Cloud-Apps.

Tipps

- Umgehende Aktualisierungen zur Schliessung von Lücken und regelmässiges Einspielen von Updates
- Sicherstellen von regelmässigen Datensicherungen (AGB's der Cloudanbieter kennen)
- Backups und entsprechende Daten nicht nur in Cloud-Diensten speichern sofern möglich
- Informieren über die Risiken der Anwendungen (Programme, Systeme, Softwareapplikationen, Apps)
- Schulung und Sensibilisierung im Umgang mit den heutigen digitalen Mitteln in der Cloud

Mobile Geräte / Mobile Apps

Mobile Apps verursachen oft ungewollte Datenlecks. So stellen beispielsweise Riskware-Apps ein echtes Problem für mobile Benutzer dar, die ihnen umfangreiche Berechtigungen zuweisen, aber nicht die Sicherheit überprüfen. Hierbei handelt es sich in der Regel um kostenlose Apps, die zwar die beworbene Funktion erfüllen, aber auch private Daten – und damit potenziell Daten Ihres Unternehmens – an Remote-Servern senden, wo sie von Werbeunternehmen oder sogar Kriminellen abgerufen werden.

Datenlecks entstehen oft durch böswillige unternehmenssignierte mobile Apps. Hier nutzen mobile Malware die Verbreitung nativer Codes beliebter Betriebssysteme, wie z.B. iOS und Android, um wertvolle Daten über Unternehmensnetzwerke hinweg zu übertragen, ohne Verdacht zu erregen.

Um dieses Problem zu vermeiden, sollten Sie Apps nur die Berechtigungen zuweisen, die absolut notwendig sind, und Apps, die mehr fordern, ignorieren. Zurzeit sehr verbreitet sind in diesem Zusammenhang Tracking-Apps, die anzeigen, wo Covid-19-Erkrankte wohnen oder unterwegs sind. Kriminelle versuchen, Anwenderinnen und Anwendern angebliche Covid-19-Tracker unterzujubeln – mit dem Ziel, Schadsoftware vom Banking- bis zum Verschlüsselungstrojaner auf Smartphones und Tablets zu schleusen. Wer solche Apps aus zweifelhaften Quellen lädt, dem drohen Kontoplünderung oder ein blockiertes Mobilgerät mit Lösegeldforderung.

Tipps

- Smartphone regelmässig mit den neuesten Updates versehen
- Anwendungen nur aus den offiziellen App-Stores installieren
- Weisen Sie Apps nur die Berechtigungen zu, die absolut notwendig sind, und Apps, die mehr fordern, ignorieren
- Für Unternehmen, in denen Dutzende oder Hunderte von Android- oder iOS-Endgeräte im Einsatz sind, ist es sinnvoll, eine zentrale Management-Konsole beziehungsweise MDM-Software für die Verwaltung der Systeme einzusetzen
- Erstellen Sie ein Sicherheitskonzept nach welchem Konfigurationseinstellungen und unternehmensweite Sicherheitsregeln definiert sind

Advantis Versicherungsberatung AG
Buckhauserstrasse 17
8048 Zürich

Neo One AG
Grindelstrasse 6
8303 Bassersdorf

Zugriff bei Endgeräten mittels SSL VPN

Bei Endgeräten, welche durch den Betrieb direkt verwaltet und zur Verfügung gestellt werden, ist das Risiko minimal. Vorausgesetzt es wird eine zentrale Antiviren-Lösung eingesetzt, welche auch auf Verschlüsselungstrojaner und neue Bedrohungen ausgerichtet ist.

Bei Installationen auf den privaten Geräten von Mitarbeitenden muss das Gerät genau geprüft und ein Virenschutz installiert werden. Wenn über diesen Kanal ein «verseuchtes» Gerät auf Firmen-Ressourcen zugreift, kann dies den Betrieb, trotz aktueller Sicherheitssysteme, evtl. kurzfristig schwächen. Zudem sollte dieses private Gerät auch in Sachen Updates auf dem neusten Stand sein. Somit werden auch im privaten Bereich potenzielle Sicherheitslücken geschlossen, welche sich sonst auf das Firmennetzwerk ausweiten könnte.

Tipps

- Mindestverschlüsselung durch einen externen Zugriff auf ein Firmennetzwerk ist die SSL-Verschlüsselung via VPN-Zugriff
- Planen und führen Sie regelmässige Sicherheitsupdates und Wartungen durch
- Exakte Einhaltung von Sicherheitsstandards für Home Office Infrastrukturen
- Gewährleistung von allen Schutzmassnahmen für jeden Home Office Zugriff und jedes Endgerät
- Achten Sie auf ganzheitliche Sicherheitskonzepte. Sicherheitskonzepte müssen alle relevanten Unternehmensbereiche umfassen. Sicherheit heisst: Informatiklösungen, Webplattformen und Digitale Systeme aufeinander abzustimmen.

Sichere Verbindung zum Firmennetzwerk / Multifaktorauthentifizierung

Unternehmen sollten Verbindungen zu Ihren Firmennetzwerken ausschliesslich über einen sicheren Fernzugang lancieren, wie ein virtuelles privates Netzwerk (VPN) oder ein anderes verschlüsseltes Verbindungsverfahren.

Zur Erhöhung der Sicherheit sollte die VPN-Verbindung mit einer Multifaktoren- bzw. 2-Faktor-Authentifizierung zusätzlich konfiguriert sein. Hier wird zusätzlich zum Passwort bei jedem Login-Vorgang eine weitere Authentifikation verlangt, wie beispielsweise ein Code per SMS oder ein Code, der über eine spezielle App bezogen werden kann. Die viel höhere Sicherheit ist einerseits durch diesen zusätzlichen Code wie auch durch die zeitliche Beschränkung des Codes garantiert.

Um mit der 2-Faktor-Authentfizierung arbeiten zu können, brauchen Sie lediglich eine App. Es gibt verschiedene Anbieter diesbezüglich, welche empfohlen werden können.

Tipps

- Erhöhung des Sicherheitslevels durch eine 2-Faktor-Authentifizierung
- Schützen Sie so viele Zugriffe wie möglich mit der 2-Faktor-Authentifizierung
- Stellen Sie in Ihrem Betrieb Richtlinien auf

Empfehlungen zur Risikoüberwälzung

Auch die bestgesicherte IT und die oben genannten Tipps zur Risikominderung schützen Unternehmen nicht zu 100%. Der Faktor Mensch ist ebenfalls nicht zu vernachlässigen und stellt in der Regel das schwächste Glied in der IT-Sicherheit dar.

Um die Restrisiken zu überwälzen und finanzielle Verluste weitestgehend zu vermindern besteht die Möglichkeit, eine Cyber-Risk Versicherung abzuschliessen. Eine solche deckt in Fällen von Cyberkriminalität u.a. folgende Bereiche ab:

Eigenschäden, welche ein Betrieb durch ein versichertes Ereignis erleidet:

- Wiederherstellungskosten von Daten und Programmen
- Notifizierungskosten (Benachrichtigungskosten betroffener Personen)
- Krisenmanagementkosten (forensische Experten, Rechtsanwälte, etc.)
- Kosten aus Cyber-Erpressung
- Entgangener Gewinn während des Unterbruches
- Mehrkosten als direkte Folge einer Unterbrechung
- PR-Kosten
- Belohnungszahlungen

Haftpflichtschäden

Den Versicherten wird Versicherungsschutz gewährt, wenn sie aufgrund einer Pflichtverletzung für einen Vermögensschaden aufgrund gesetzlicher Haftung erstmals auf Schadenersatz in Anspruch genommen werden.

- Ansprüche infolge Datenschutzverletzungen
- Ansprüche infolge Persönlichkeitsrechtsverletzungen (nach einem Datenverlust)
- Ansprüche infolge Verletzung des geistigen Eigentums
- Ansprüche infolge Übermittlung von Malware auf Drittsysteme

Gerne steht Ihnen Ihr Advantis-Team und Neo One für Fragen rund um Cyber Risiken und Versicherungen zur Verfügung.

Advantis Versicherungsberatung AG
Buckhauserstrasse 17
8048 Zürich

Neo One AG
Grindelstrasse 6
8303 Bassersdorf

Gut zu wissen

SSL-Verschlüsselung

Bei SSL (Secure Socket Layer) handelt es sich um ein Verschlüsselungsprotokoll zur Datenübertragung im Internet bzw. um eine verschlüsselte Netzverbindung zwischen Server und Client, über die auch unverschlüsselte Anwendungsprotokolle (z.B. HTTP, POP3, IMAP, SMTP, NNTP, SIP, ...) sicher transportiert werden können.

VPN-Zugriff

Das konventionelle VPN bezeichnet ein virtuelles privates Kommunikationsnetz. Virtuell in dem Sinne, dass es sich nicht um eine eigene physische Verbindung handelt, sondern um ein bestehendes Kommunikationsnetz, das als Transportmedium verwendet wird.

Backup

Backup/Datensicherung bezeichnet das Kopieren von Daten in der Absicht, diese im Falle eines Datenverlustes zurückkopieren zu können. Somit ist Datensicherung eine elementare Massnahme zur Datensicherheit. Die auf einem Speichermedium redundant gesicherten Daten werden als Sicherungskopie «Backup» bezeichnet.

Cloud

Cloud ist eine IT-Infrastruktur (Rechenzentren), die über das Internet verfügbar gemacht wird. Sie beinhaltet in der Regel Speicherplatz, Rechenleistung oder Anwendungssoftware als Dienstleistung.

Maillog

Eine Log-Datei ist eine Datei, in der IT-Systeme Ereignisse eintragen und protokollieren. Die Datei soll helfen, bestimmte Vorgänge nachzuvollziehen und kann beispielsweise für die Problemanalyse oder die Rekonstruktion von Transaktionen zum Einsatz kommen. Die Log-Datei ist in der Regel textbasiert.

Die Autoren

Mirco Vivarelli
Mitglied der Geschäftsleitung
Advantis Versicherungsberatung AG

Jan Braunschweiler
Inhaber & Geschäftsführer
Neo One AG

Josef Neubauer
Mandatsleiter Unternehmenskunden / Teamleiter
Advantis Versicherungsberatung AG

Ronny Troxler
ICT Consultant & Senior ICT System Engineer
Neo One AG

Advantis Versicherungsberatung AG
Buckhauserstrasse 17
8048 Zürich

Neo One AG
Grindelstrasse 6
8303 Bassersdorf