PROXESS® Whitepaper

Vernetzte Welt - sichere Welt?

Wie Sie Ihr Unternehmen vor Cyberattacken schützen können

Inhaltsverzeichnis

Auch „sichere“ DMS-Systeme müssen vor Cyberattacken geschützt werden

Wir werden schneller, mobiler, smarter. Gleichzeitig nimmt der Grad der digitalen Vernetzung nicht nur im privaten Umfeld, sondern auch beim Einsatz von IT-Systemen in Unternehmen und Behörden zu. Nahezu alle Prozesse setzen dabei den Austausch von Daten - auch über die Grenzen des eigenen Arbeitsumfeldes hinweg - voraus. Parallel dazu steigt weltweit die Anzahl der berichteten Cyber-Vorfälle, die mitunter für Firmen und Behörden ernsthafte Konsequenzen haben. Ein wesentliches Risiko ging in letzter Zeit dabei laut aktuellem „Lagebericht zur IT-Sicherheit“ des Bundesamtes für Sicherheit in der Informationstechnik (BSI) von der Schadsoftware „Emotet“ aus.

3 von 4 Unternehmen sind betroffen

In einer aktuellen bitkom-Umfragestudie „Spionage, Sabotage und Datendiebstahl - Wirtschaftsschutz in der vernetzten Welt“ aus dem Jahr 2020 geben 3 von 4 Unternehmen an, dass sie in den vergangenen zwei Jahren von Datendiebstahl, Industriespionage oder Sabotage betroffen oder vermutlich betroffen waren. In den bitkom-Umfragen von 2017 und 2015 waren es nur gut jedes zweite Unternehmen.

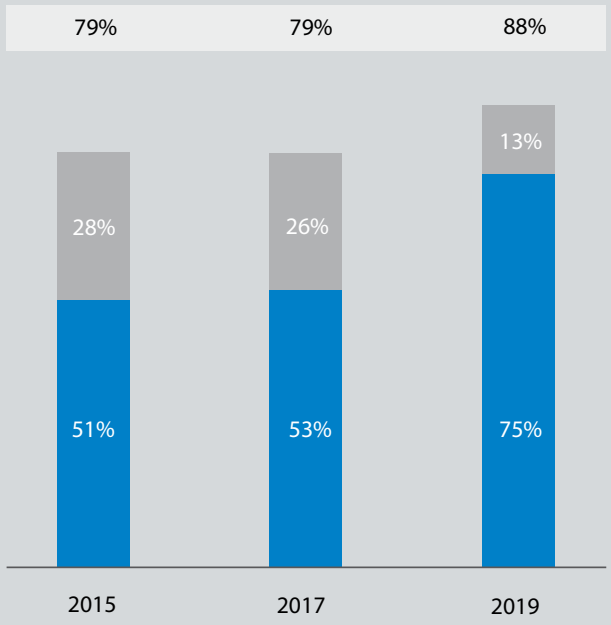
Hierzu meint Heinz Pretz, Leiter Softwareentwicklung und Kundenservice bei der PROXESS GmbH: „Auch einige unserer Kunden sammelten bereits schmerzvolle Erfahrungen mit Cyberattacken. Hier waren jeweils auch die Server betroffen, auf denen unsere Dokumentenmanagementsysteme (DMS-Systeme) installiert waren. Trotz eines integrierten, dreistufigen Sicherheitskonzepts für die Daten unserer Softwarelösungen kann ein DMS-System keinen Schutz vor einem Virenbefall oder Serverdefekt an sich bieten. Zwar arbeitet unser DMS-System ohne Netzwerkfreigaben, die ja ein typisches Einfallstor für Schadsoftware darstellen. Doch oft sind Netzwerkfreigaben aus anderen Gründen auf den Servern eingerichtet. Daher müssen nach unserer Erfahrung meist auch die im DMS-System archivierten Daten - sieht man einmal von den Daten ab, die auf externen und bestenfalls schreibgeschützten Medien ausgelagert sind - im Desaster-Fall über entsprechende serverseitige Backups wiederhergestellt werden.“

Heinz Pretz,
Leiter Softwareentwicklung und Kundenservice

PROXESS GmbH

„Auch einige unserer Kunden sammelten bereits schmerzvolle Erfahrungen mit Cyberattacken. Hier waren jeweils auch die Server betroffen, auf denen unsere Dokumentenmanagementsysteme (DMS-Systeme) installiert waren. Trotz eines integrierten, dreistufigen Sicherheitskonzepts für die Daten unserer Softwarelösungen kann ein DMS-System keinen Schutz vor einem Virenbefall oder Serverdefekt an sich bieten.

Auch die im DMS-System archivierten Daten - sieht man einmal von den Daten ab, die auf externen und bestenfalls schreibgeschützten Medien ausgelagert sind - müssen im Desaster-Fall über entsprechende serverseitige Backups wiederhergestellt werden.“



War Ihr Unternehmen innerhalb der letzten 2 Jahre von Datendiebstahl, Industriespionage oder Sabotage betroffen?

Vermutlich betroffen
Betroffen
Gesamt

Basis: Alle befragten Unternehmen (2019: n=1.070; 2017: n:1069; 2015: n=1074)
Quelle: Bitkom Research

Grund genug für uns, dieses Thema einmal ausführlich anzusprechen. In diesem Whitepaper haben wir uns mit Experten im Bereich Cybersecurity unterhalten. Diese geben einen Überblick über die größten Gefahren und erläutern, welche Maßnahmen für Unternehmen sinnvoll sind, um sich effektiv vor Cyberattacken zu schützen oder zumindest deren Folgen abzumildern. Silvana Rößler ist Expertin für Digitale Forensik und unterstützt gemeinsam mit ihrem Team von der networker, solutions GmbH betroffene Unternehmen bei der Analyse und bei der Abwehr bzw. Schadensbegrenzung von Informationssicherheitsvorfällen aus forensischer Sicht. Oftmals nimmt das Team dabei die Rolle eines „Gutachters" bei Cyberattaken ein.

Vielen Unternehmen ist die Möglichkeit, sich gegen Cyberrisiken zu versichern, noch nicht ausreichend bekannt. Daher möchten wir diese Möglichkeit hier einmal vorstellen. Dirk Kordus und Matthias Neumann - beides Versicherungsexperten der Cogitanda Group - erläutern, welche Voraussetzungen bei Unternehmen vorliegen müssen, was versichert werden kann und wie man als Unternehmen im Schadensfall am besten agiert.

Sicherheit muss gelebt werden

Wenn man die Wirkweise einer Schadsoftware wie Emotet betrachtet wird deutlich, wie vielschichtig die notwendigen Schutzmaßnahmen in Unternehmensnetzwerken sein müssen. Ein wichtiger Aspekt dabei ist, dass viele Schutzmaßnahmen noch nicht einmal mit hohen Investitionen verbunden sind, sondern rein organisatorischer Natur sind. Denn die technische Vorsorge allein kann keine hundertprozentige Sicherheit für Ihre Daten bieten. Technik sollte eine solide Basis bilden – Sicherheit muss jedoch auch gelebt werden! Dabei wird in der Praxis immer wieder klar: „Luxus" steht bei der Arbeit mit EDV-Systemen oft im Widerspruch zur Sicherheit. Überall dort, wo unsinnige Automatisierung (Wird das tägliche Backup wirklich kontrolliert oder begnügt sich der Administrator mit einer Quittungsmail à la „Backup erfolgreich"?) Einzug hält oder wo aus Bequemlichkeit auf sinnvolle Sicherheitsvorkehrungen (Wie ist bei Ihnen eine Passwortrichtlinie umgesetzt?) verzichtet wird, entstehen potentielle Sicherheitslücken.

Wichtige Cyberschutz To Do´s - wo steht mein Unternehmen?

Sowohl technische als auch organisatorische Aspekte sowie auch deren Umsetzung beeinflussen das Schadensrisiko bei einem Cyberangriff in Ihrem Unternehmen entscheidend. Mit unserem Fragenkatalog zur Selbstkontrolle im Anhang können Sie schnell Ihr eigenes aktuelles Sicherheitsniveau abschätzen. Auch, wenn eine solche Grobabschätzung keinen Anspruch auf Vollständigkeit erhebt, haben sich die hier angesprochenen Punkte in der Praxis als wichtige und gleichzeitig schnell umsetzbare Hebel erwiesen.

Eine aktuelle Datensicherung ist immer noch das A und O

Sollte eine Schadsoftware wie Emotet bereits ausgebrochen sein, ist ein Daten-Backup letztlich die einzige Rettung. Die oftmals mit Verschlüsselungstrojanern einhergehenden Erpressungen sind nicht mehr als eine Masche. Auf eine Rettung der Daten kann man in den meisten Fällen auch bei Bezahlung eines „Lösegeldes" nicht hoffen. Daher ist man grundsätzlich gut beraten, wenn ein möglichst „frisches" Daten-Backup zur Hand ist. Wie lange würde es in Ihrem Netzwerk dauern, alle Server aus einem Backup wiederherzustellen und die Benutzer-PCs neu zu installieren? Ein Szenario, das Realität wird, wenn Emotet zuschlägt.

Sind alle PCs mit einem Virenschutz versorgt? Sind sie auf einem vertretbaren Patch-Level? Wie sind die Einstellungen der Personal-Firewall der Geräte? Damit das Risiko eines solchen Ausbruchs sinkt, sind diese einfachen technischen Vorkehrungen unabdingbar. Auch, wenn die Anforderungen und Fragen simpel anmuten, gilt es, weiterhin zu hinterfragen: Wer kontrolliert diese drei Aspekte für jedes Gerät? Sind die entsprechenden Einstellungen zentral gemanagt? Sind diese Vorkehrungen auch noch gewährleistet, wenn sich ein Mitarbeiter aus dem Homeoffice per VPN in das Firmennetzwerk einwählt?

Corona schafft weitere Einfallstore für Schadsoftware und Viren

Gerade in der aktuellen (Corona-)Zeit erleben Firmennetzwerke durch Änderungen der Arbeitsweise der Belegschaft wie Homeoffice massive strukturelle Änderungen. Zugänge z. B. über VPN oder Terminalserver werden oft unter Zeitdruck geschaltet.

Dadurch wird der sogenannte „Perimeterschutz" des Netzwerks aufgeweicht. In diesem Moment reicht der herkömmliche (Router-)Firewallschutz nicht mehr, da nun plötzlich schon an der ersten Abgrenzung Ihres Netzwerks zum Internet mit höherwertigeren Sicherheitsfunktionen gearbeitet werden muss. Übrigens: Auch eine Kontrolle des Datenverkehrs innerhalb Ihres Netzwerks ist heutzutage kein Hexenwerk mehr. Funktionen wie „deep packet inspection" (DPI) oder ein „intrusion detection system" (IDS) waren noch vor ein paar Jahren sehr teure Netzwerk-Hightech-Komponenten. Mittlerweile sind diese Funktionen oft schon in höherwertige Netzwerkkomponenten (Switches, Firewalls, ...) integriert – und funktionieren sehr gut.

Der Faktor „Mensch" wird oftmals unterschätzt

All diese technischen Maßnahmen können allerdings nur unterstützen. Die Daten, die zu einem hohen Prozentsatz nicht-automatisiert generiert werden und gegebenenfalls auch aus unbekannten Quellen stammen, müssen letztlich doch von Menschen verarbeitet werden. Und genau hier liegt das höchste Gefahrenpotential für einen Cybervorfall. Sind Ihre Mitarbeiter ausreichend geschult und sensibilisiert, wenn Sie mit externen Daten umgehen?

Die berühmte, schon oft zitiere E-Mail mit der virenverseuchten Dateianlage ist hier aber nur der erste Schritt einer Betrachtung der Komponente „Mensch". Der interne IT-Beauftragte, der dem Mitarbeiter, der die genannte Dateianlage geöffnet hat und dessen PC jetzt „spinnt", zu Hilfe eilt, bildet gleich das nächste Kettenglied. Er will den Fehler korrigieren, meldet sich dazu mit seinen Administrator-Rechten am PC des Mitarbeiters an. Und schon jetzt nimmt das Virus im Netzwerk Fahrt auf. Leicht wäre es, dem EDV-Beauftragten nun die Schuld am entstandenen Desaster zu geben. Aber war er wirklich auf diese Situation vorbereitet?

Die Grenzen zwischen privatem und dienstlichem IT-Umfeld verschwimmen zunehmend

Ein letzter „menschlicher" Faktor ist das sogenannte „social engineering". Hiermit ist längst nicht nur der Mitarbeiter gemeint, der dem „neuen Admin" am Telefon auf den Leim geht und freiwillig seine Passwörter nennt. In Zeiten, in denen Social Media einen wichtigen Platz in unserem Leben und in unserem Arbeitsalltag einnimmt und wir fast schon einen 24-Stunden währenden „Smartheitsgrad" erreicht haben, muss dringend eine Grenze zwischen Job und Privatem gezogen werden. Damit ist auch eine technische Grenzziehung gemeint. WhatsApp ist auf einem Diensthandy zusammen mit Daten und Kontakten aus dem Arbeitsumfeld einfach nicht vertretbar. Wer noch nie über den Namen „Robin Sage" gestolpert ist, der sollte ihn dringend einmal googeln.

Wann enstehen die größten Schäden und wie verhalte ich mich bei einer Cyberattacke richtig?

Frau Rößler, welche Art Malware - wenn man das pauschal sagen kann - ist für Firmen die bedrohlichste? Wann entstehen die größten Schäden?

Jede Malware, die es schafft, in ein Unternehmensnetzwerk einzudringen und aktiv zu werden, stellt für Unternehmen ein Risiko dar. Das Ausmaß des durch die Schadsoftware verursachten Schadens hängt aber von dem Typ der Malware, den infizierten Geräten und der auf den Geräten gespeicherten Informationen ab.

Während einige Schadprogramme, wie Cryptominer oder Trojaner zum Spamversand, es nur auf die Ressourcen der befallenen Geräte abgesehen haben und keine erhöhte Gefahr für den Betriebsablauf darstellen, können andere Schadprogramme schwerwiegende Auswirkungen auf das Unternehmen haben. Hierzu zählt der Ausfall des Unternehmensnetzwerks, der Datenverlust oder auch der Informationsabfluss.

Aktuelle Bedrohungen stellen hier Verschlüsselungstrojaner dar. Diese kommen in verschiedenen Variationen vor und können für die betroffenen Unternehmen einen sehr hohen finanziellen und auch einen Reputationsschaden bedeuten. Ein Verschlüsselungstrojaner (auch Ransomware genannt), welcher durch eine Schwachstelle ins Netzwerk gelangen konnte, besitzt die Möglichkeit, sich selbst in diesem zu verbreiten und sämtliche Dateien, auf die er Zugriff erlangen kann, zu verschlüsseln. Das können wichtige Daten oder auch Datensicherungen sein, die sich im Netzwerk befinden. In den überwiegenden Fällen wird bei den verschlüsselten Dateien eine Lösegeldforderung hinterlassen. Eine eigenständige Entschlüsselung der Daten ist bei diesem Typ Malware nahezu unmöglich. In diesem Fall hilft nur noch das Rückspielen von funktionstüchtigen

Silvana Rößler, Head of Security Incident Response

networker, solutions GmbH

Dipl. Inform. (FH) Silvana Rößler, MSc. Digitale Forensik und ihr Team bei der networker, solutions GmbH unterstützen Unternehmen bei Informationssicherheitsvorfällen.

Als Experten für Incident Response und Digitale Forensik sowie IT-Sachverständige ist es ihnen möglich, durch technische Analyse betroffener Systeme computergestützte Angriffe zu erkennen, diese einzudämmen, zu stoppen und aufzuklären.

Die oft schwer nachvollziehbaren Spuren können so gerichtsverwertbar gesichert, nachverfolgt und anschließend im Rahmen der Strafverfolgung als Beweismittel eingesetzt werden.

Aber auch die präventive Beratung, Schulungen, Fachvorträge sowie Live-Hacking Veranstaltungen rund um die Informationssicherheit profitieren von den langjährigen Erfahrungen der Experten.

Datensicherungen. Ist ein Backup nicht vorhanden oder lässt es sich nicht zurücksichern, bleibt oftmals nichts anderes übrig, als das geforderte Lösegeld zu bezahlen.

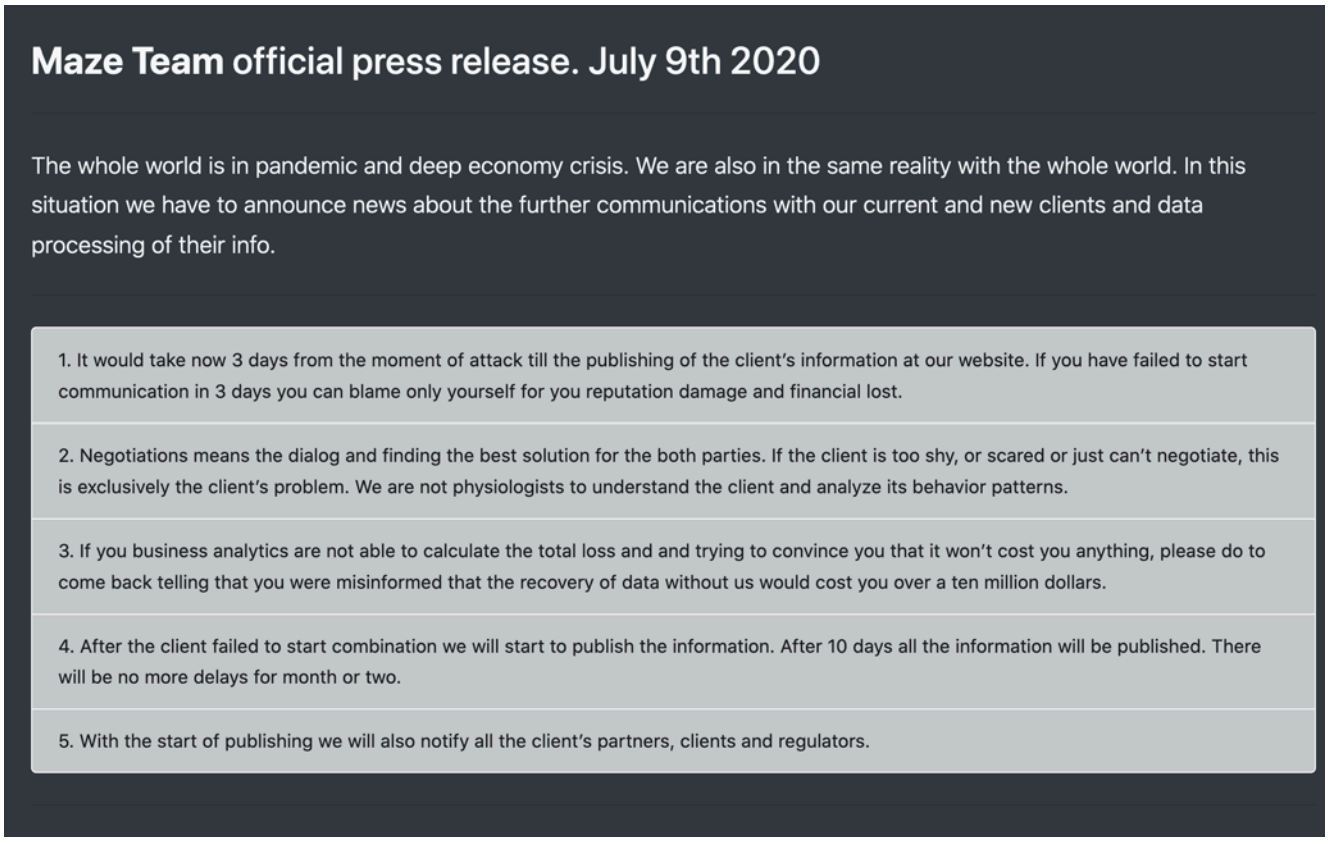
Verschlüsselungstrojaner benötigen jedoch immer eine Schwachstelle, über die sie ein Netzwerk befallen können. Das können nicht ausreichend abgesicherte Fernzugänge, veraltete Betriebssysteme oder fehlende Updates sein.

Aber auch Mitarbeiter, welche Anhänge einer infizierten Mail öffnen oder eine Datei von einer kompromittierten Webseite herunterladen stellen oftmals ein beliebtes Einfallstor für Angreifer dar.

Wurde erst einmal ein Weg in das System gefunden, können verschiedene Schadprogramme nachgeladen werden. Dieser Methode bedient sich beispielsweise Emotet. Ist ein Computer mit diesem Trojaner infiziert, lädt dieser unbemerkt weitere Schadsoftware, wie den Banking-Trojaner Trickbot oder QBot nach. Bei vielen infizierten Systemen konnte festgestellt werden, dass Antivirenprogramme durch die Trojaner deaktiviert wurden oder diese nicht entfernen konnten. Ist Emotet auf einem Computer aktiv, liest er die Kontaktbeziehungen und E-Mail-Inhalte aus den Postfächern der infizierten Systeme aus. Diese werden von den Tätern genutzt, um authentisch aussehende Kommunikation zu generieren, die an die Kontakte des Opfers versandt werden, um weitere Unternehmen zu infizieren. Trojaner dieser Kategorie führen zu Datenabfluss oder ermöglichen den Kriminellen eine vollständige Kontrolle über die Systeme. Haben die Täter unbemerkt alle Informationen abgezogen, folgt in vielen Fällen ein Verschlüsslungstrojaner, der die befallenen Systeme verschlüsselt und eventuell im Netzwerk gespeicherte Datensicherungen unwiderruflich löscht.

Selbst wenn das Lösegeld nicht beglichen werden muss, da eine Wiederherstellung der Systeme mittels Offline-Backups möglich ist, haben diese Angriffe große Betriebsunterbrechungen und Produktionsausfälle zur Folge, da ganze Unternehmensnetzwerke neu aufgebaut werden müssen.

Die momentan gefährlichste Art der Bedrohung stellen jedoch Verschlüsselungstrojaner mit doppelter Erpressung, wie beispielsweise MAZE, Doppelpaymer, Cl0p oder Sodinokibi dar. Haben diese Zugang zu einem Unternehmensnetzwerk gefunden,



kopieren die Angreifer unbemerkt sensible Unternehmensinformationen und – kommunikationen, statt lediglich die Daten zu verschlüsseln und drohen anschließend, bei Nichtzahlung des Lösegeldes, mit deren Veröffentlichung. Gehen die erpressten Unternehmen nicht auf die Lösegeldforderung, welche oftmals im Millionenbereich liegt, ein, so werden diese sensiblen Informationen im Darknet veröffentlicht. Wird eine Veröffentlichung der Daten in Kauf genommen, kann dies Reputationsverluste und ein Abfluss erfolgskritischer Informationen bedeuten. Ob das Lösegeld gezahlt wird oder nicht, in beiden Fällen ist es erforderlich, dass das ganze Unternehmensnetzwerk neu aufgebaut wird, da dieses als kompromittiert anzusehen ist. Dies bedeutet für das Unternehmen in jedem Fall eine kostspielige Betriebsunterbrechung. Auch ist es nach einem Trojanerbefall dringend notwendig, dass in Zusammenarbeit mit IT-Forensikern untersucht wird, auf welchem Weg der Trojaner in das Netzwerk gelangen konnte. Denn nur so kann diese Sicherheitslücke für zukünftige Angriffsversuche geschlossen werden.

Welche Gegenmaßnahmen sollten Firmen am dringlichsten ergreifen?

Hier gilt an erster Stelle immer der Grundsatz: Informationssicherheit ist Chefsache! Wie in der vorhergehenden Frage erläutert, kann ein Cyberangriff sehr schnell zu einer finanziellen Schieflage eines Unternehmens führen. Daher ist es wichtig, dass rechtzeitig umfassende Analysen erfolgen und Maßnahmen umgesetzt werden. So ist von zentraler Bedeutung, die wichtigsten und sensibelsten Informationen eines Unternehmens sowie ihren Speicherort zu ermitteln. Hierbei sollte sich ein Unternehmer die Frage stellen, welche Auswirkungen es für sein Unternehmen hat, wenn diese Daten und Systeme durch einen Angreifer kompromittiert werden. Dementsprechend müssen auch die jeweils angepassten Maßnahmen zum Schutz dieser Informationen ergriffen werden.

Die grundlegenden Maßnahmen sind von jedem Unternehmen umsetzbar. Dazu gehören der ausschließliche Einsatz aktueller Betriebssysteme mit aktuellstem Updatestand sowie der Einsatz von Antivirensystemen. Sollten Fernzugriffe, wie Remote-Desktop-Zugänge notwendig sein, müssen diese fachgerecht abgesichert werden. Administratoren-Accounts mit weitreichenden Berechtigungen dürfen nur Administratoren für entsprechende Tätigkeiten vorenthalten sein. Eine gern von Angreifern ausgenutzte Schwachstelle stellen einfache Passwörter dar. Bei einer Vielzahl der Angriffe stellen wir fest, dass immer noch zu kurze Passwörter oder leicht zu erratende Passwörter, wie Vornamen oder Firmenbezeichnungen genutzt werden. Diese schrecken Angreifer nicht ab und halten sie nicht von den Systemen fern. Um die Angriffsfläche „Mitarbeiter" oder „Mensch" zu reduzieren, empfehle ich regelmäßige Schulungen für Mitarbeiter. Ein Mitarbeiter, welcher weiß, wie er eine Phishing-E-Mail erkennt und das Wissen anwenden kann, wird den Trojaner nicht herunterladen und aktivieren.

Die absolut wichtigste Maßnahme in einem Unternehmen jedoch stellen Datensicherungen dar. In vielen unserer aussichtslos erscheinenden Fälle waren Datensicherungen, welche offline (also nicht am System – z. B. Bänder in einem Safe) vorlagen, die letzte Rettung. Und keine Situation ist für alle Beteiligten schlimmer, als wenn sich diese Datensicherung als defekt darstellt.

Daher rate ich dringend jedem Unternehmen, das IT-Systeme einsetzt:

Ermitteln Sie, wo Ihre wichtigen Informationen gespeichert sind.

Überprüfen Sie Ihr Backup-Konzept. Werden alle unternehmenskritischen und relevanten Daten gesichert?

Wie oft werden diese gesichert? Wohin werden diese gesichert?

Wenn Sie Ihre Datensicherung auf einem Netzwerkspeicher, wie einem NAS-System speichern, stellen Sie sicher, dass auch eine Kopie der Datensicherung auf ein Offline-Medium vorgenommen wird und weg-

geschlossen wird.
Denken Sie daran: Was nicht am Netzwerk hängt, kann nicht durch einen Angreifer gelöscht oder verändert werden. Überprüfen Sie in regelmäßigen Abständen, ob und wie die Backups wiederherstellbar sind.

Dokumentieren Sie Ihr Netzwerk, Ihre IT-Systeme, notwendige Zugänge und Wiederherstellungs- und Wiederanlaufreihenfolgen und sichern Sie diese Informationen so, dass Sie auch bei einem kompletten IT-Ausfall auf diese zugreifen können. Besprechen Sie mit Ihrem IT-Betreuer, dass dieser auch im Fall eines Angriffs oder eines IT-Ausfalls erreichbar ist – Hacker kennen keinen Feierabend! Lassen Sie in regelmäßigen Abständen Ihre Prozesse und Systeme von Sicherheitsberatern überprüfen, denn Informationssicherheit ist ein immer fortlaufender Prozess.

Macht eine polizeiliche Anzeige bei einem Cybervorfall Sinn? Können polizeiliche Ermittlungen überhaupt greifen?

Jede polizeiliche Anzeige eines Angriffs macht Sinn. Sie müssen sich vorstellen, ein Einbrecher dringt in Ihre Wohnung ein und fotografiert sensible Dokumente, um Sie danach damit zu erpressen – oder er sperrt Sie aus Ihrer Wohnung aus. In diesem Fall würden Sie nicht lange zögern und die Polizei zu Hilfe holen. So ist es auch mit Ihrem Netzwerk - sehen Sie es wie Ihr digitales Heim. Auch wenn sich hierbei neue technische und rechtliche Herausforderungen ergeben ist es wichtig, dass Opfer von Cyberangriffen diese melden, so dass diese verfolgt werden können. Man muss bedenken, dass eine Erpressung – egal in welcher Höhe – eine Erpressung bleibt. Wir haben bisher durchweg positive Erfahrungen in der Zusammenarbeit mit den Kollegen der Strafverfolgungsbehörden.

Ein vorhandenes Backup ist für die Wiederherstellung der Arbeitsfähigkeit eines Unternehmens unerlässlich. In jüngerer Zeit ist dies im Fall eines Erpressungsversuchs allerdings nur die halbe Miete. Oft wird gleichzeitig mit der Veröffentlichung von zuvor abgezogenen Daten gedroht. Wie verhalte ich mich richtig?

Hierbei handelt es sich um die doppelte Erpressung. Zuerst ist es wichtig, wie bei jedem Angriff, Ruhe zu bewahren, Spezialisten, wie IT-Forensiker zu konsultieren und die Strafverfolgungsbehörden zu informieren. Diese benötigen Sie für die Kommunikation mit den Erpressern sowie bei einer eventuell notwendigen Lösegeldzahlung.

Hat man eine Cyberversicherung abgeschlossen, bekommt man auf diesem Weg unkompliziert und schnell Hilfe durch geschulte Fachkräfte. Im besten Fall kann festgestellt werden, wie der Trojaner in das System gelangt ist und welche Systeme kompromittiert wurden. Dies dient zur Einschätzung des Umfangs des Datenabflusses. Anschließend kann mit allen Beteiligten eine Kommunikationsstrategie und der Wiederaufbau des Unternehmens geplant werden. Gerade in einer solchen Krise ist es wichtig, verlässliche und vertrauenswürdige Partner an der Hand zu haben.

Eine Cyberversicherung kann häufig das Schlimmste abwenden - nicht nur finanziell

Herr Kordus, das BSI hatte in seinem letzten Bericht „Die Lage der IT-Sicherheit“ von 2019 wieder einen deutlichen Anstieg der Cybervorkommen ausgewiesen. Der Anstieg war damals nicht mehr so stark wie in den Vorjahren, aber dennoch deutlich. Haben Sie über Ihre Fallzahlen eine Einschätzung zur aktuellen Lage in 2020?

Wir sind als Versicherer seit Anfang 2018 mit einer speziellen Versicherung für Cyberrisiken auf dem Markt. In diesem Zeitraum konnten wir ein überproportionales Schadenswachstum feststellen. Besonders Emotet hat uns im letzten Jahr eine Vielzahl neuer Schadensfälle „eingebracht“. In diesem Jahr stellen wir häufig fest, dass neben der Verschlüsselung der Daten auch gleichzeitig Informationen geraubt werden, die im Anschluss im Darknet verkauft werden. Auch im Jahr 2020 steigen die Schadenstückzahlen innerhalb der COGITANDA Gruppe deutlich an, mit dem Schwerpunkt Verschlüsselungstrojaner und gleichzeitigem Datenabfluss.

Welche Schäden entstehen in den betroffenen Firmen?

Die Schäden sind sehr vielfältig. Sie reichen von einer Verschlüsselung von Daten bis zum Datendiebstahl und Erpressung in Millionenhöhe. Wir haben Schadensfälle, bei denen wir als Versicherer die Lösegeldforderung abwickeln und der Unternehmer dann sehr zeitnah wieder voll einsatzbereit ist bis hin zu Schäden, bei denen die Hardware nicht mehr einsatzbereit ist, sensible Daten wie Kundendaten und Passwörter abgeflossen sind und diese im DarkNet veröffentlicht und verkauft werden.

Dirk Kordus
Chief Claims Officer

Matthias Neumann
Chief Underwriting Officer

COGITANDA Group

Die COGITANDA Group bietet auf Wunsch jede Form von Cyberrisiko-Prävention an, von Mitarbeiterschulungen über Audits bis hin zu Hard- und Softwarelösungen zum Schutz vor Cyberangriffen. Auch bei der Durchführung der identifizierten Maßnahmen, kann auf Experten der COGITANDA zurückgegriffen werden.

Darüber hinaus können durch Cyberangriffe z. B. auch Sachwerte aller Art bei einem Unternehmen zerstört und Menschenleben gefährdet werden.

Herr Neumann, können Sie uns den Vorgang bis zum Abschluss einer solchen Versicherung bei Ihnen kurz beschreiben?

Vor dem eigentlichen Abschluss einer Versicherung stehen die Risiko-Beratung und die positive Beeinflussung von Sicherheitsrisiken. Versichert wird dann das verbleibende Risiko. Da es sich bei Cyberrisiken um hochkomplexe und vielschichtige Risiken handelt, ist eine ganzheitliche Betrachtung und Risikobewertung zwingend erforderlich.

Hierzu zählen insbesondere Präventionsmaßnahmen. Trotz einer vielleicht sehr gut aufgestellten IT-Sicherheit, bleibt regelmäßig ein nicht unerhebliches Risiko vorhanden. Die Eintrittswahrscheinlichkeit eines Cyberschadens kann durch geeignete Maßnahmen reduziert werden – ausschließen lässt sich der Eintritt aber nicht. Der Abschluss einer Cyberversicherung dient immer dazu, die Folgen eines Schadens für das Unternehmen wirtschaftlich tragfähig zu machen.

Um Cyberrisiken effektiv begegnen zu können, muss vorab ein Verständnis für diese Risiken geschaffen werden. Dies erfolgt bei uns in drei Schritten.

1. Schritt: Risiken erkennen
Die Prävention beginnt mit der Erfassung und Bewertung bestehender Risiken. Nur was erkannt wurde, kann beeinflusst werden.

2. Schritt: Risiken beeinflussen
Erkannte Defizite gezielt zu beheben, technisch wie organisatorisch, wird zu einer Pflichtübung eines jeden Unternehmens, das langfristig nicht in einem Hagel von Cyberangriffen untergehen will.

3. Schritt: Training und permanente Kontrolle
Die beste Technik und die besten Prozesse helfen nicht, wenn Mitarbeiter nicht regelmäßig im Umgang mit Cyberrisiken trainiert werden.

Nach der Ermittlung der Cyberrisiken eines Unternehmens ergibt sich daraus der resultierende Versicherungsbedarf. Im Zusammenspiel mit dem Versicherungsmakler hat jedes Unternehmen bei uns die Möglichkeit, eine individuelle, auf Bausteinen basierende, Versicherungsdeckung zu erhalten. Auch die Wahl der individuellen Policenlimite sowie Selbstbeteiligungen ist dabei ein wichtiges Thema.

Die Implementierung einer vollumfänglichen Absicherung geht oft schneller als gedacht; entweder innerhalb weniger Stunden oder bei umfangreichen Risiko-Präventionsmaßnahmen innerhalb von wenigen Tagen. Dabei sind wir als Versicherer immer darauf bedacht, dass wirklich nur ein echtes Risiko versichert wird und dass der Kunde am Ende auch nur das bezahlt, was er wirklich versichert haben möchte.

Welche Voraussetzungen müssen Kunden erfüllen, damit eine Cyberversicherung bei Ihnen abgeschlossen werden kann?

Zur Bewertung der individuellen Risikosituation benötigen wir zwar einige Angaben zur aktuellen Situation des jeweiligen Unternehmens. Der Aufwand an dieser Stelle ist aber weit geringer, als viele Unternehmen zunächst glauben.

Um den Prozess des Abschlusses einer Cyberrisiko Deckung zu vereinfachen, nutzen wir einen Quotierungsprozess. Dieser enthält einige wenige, dafür aber relevante IT-Risikofragen. So stellen wir sicher, dass Versicherungsnehmer einen gewissen Grad an vorbeugenden Maßnahmen selbst initiieren und einen technischen „Grundschutz" besitzen. Weitere wichtige Angaben sind der Umsatz, die Branche, bestehende Aktivitäten im Ausland und natürlich auch die Frage, ob es schon Cybervorfälle gegeben hat. So kann man erkennen, ob der Kunde aus solchen Vorfällen gelernt hat und ob sich seine Resilienz gegen über Cyberangriffen entsprechend erhöht hat.

Wir stellen uns vor: In einer Firma macht sich ein IT-Virus breit. Keine Daten mehr vorhanden, das Netzwerk ist „tot". Die Panik - sicher nicht nur auf EDV-Abteilungsseite - steigt. Herr Kordus, wie verhält sich ein Unternehmen in dieser Situation richtig? Und wie sollte man generell im Falle eines Cyberangriffs reagieren?

Sobald ein Cyberangriff oder eine Auffälligkeit in den Systemen bemerkt wird, ist es das Wichtigste, dass das geschädigte Unternehmen seinen Versicherer unverzüglich und sofort kontaktiert. Cyberschadensfälle sind sehr zeitkritisch, jede Minute zählt hierbei, um das Ausmaß des Schadens in Grenzen zu halten und existenzbedrohende Folgen abzuwenden – da muss jeder Handgriff sitzen. Eine sofortige Kontaktaufnahme zur Hotline des Versicherers ist daher zunächst das Wichtigste.

Mit der Unterstützung von spezialisierten Forensikern können wir uns dann schnell einen Überblick über die eingetretene Situation verschaffen. Anhand dessen werden sofort Maßnahmen festgelegt und umgesetzt, um die kritische Situation zu entschärfen.

Je nach Bedarf erfolgt der Einsatz sowie die Koordination von Dienstleistern auch vor Ort. Der Kunde steht hier laufend mit uns im Austausch und wird vollständig in das Geschehen eingebunden. Wir sorgen auch dafür, dass der laufende Betrieb wiederhergestellt wird und helfen dem Kunden, sich so schnell wie möglich wieder um seine Kunden und um sein Geschäft kümmern zu können.

Fragenkatalog zur Selbstkontrolle

Backup	Sind Ihre Backups vor Zugriffen aus dem Netzwerk geschützt (also „offline“) und wären sie bei einem Ausbruch einer Schadsoftware im Netzwerk sicher gelagert? Werden regelmäßig „Disaster Recovery Tests“ durchgeführt?
Dokumentation	Existiert eine Dokumentation der IT-Landschaft? Sind unternehmenskritische Systeme definiert; existieren Wiederanlaufpläne?
Virenschutz / Sicherheitsupdates	Können Softwarestand Ihres Virenschutzes und der Patchlevel Ihrer Netzwerkgeräte zentral gemanaget werden; existiert ein Alarmierungsmechanismus? Existieren für Benutzer Richtlinien / Anweisungen beim Umgang mit Daten aus dem Internet?
Perimeterschutz	Sind Funktionsweise bzw. Sicherheitsgrad Ihrer Firewall an die Bedürfnisse Ihres Unternehmens angepasst? Wie sind Zugänge in Ihr Unternehmensnetzwerk abgesichert?
Passwortschutz	Mittlerweile raten die meisten Experten (auch das BSI) von regelmäßigen Passwortänderungen ab, diese sorgen eher für eine schleichende Kompromittierung der Komplexität. Aber: Sind die eingesetzten Passworte sicher genug, um sie auch längerfristig einzusetzen?
BYOD bzw. Anschluss von Dritten im Netwerk	Ist ein Ihrem Standard entsprechendes Sicherheitslevel (vgl. „Virenschutz/Sicherheitsupdates“) auch beim Einbringen von „Fremdgeräten“ in Ihr Netzwerk gewährleistet? Existieren Sicherheitsvorkehrungen wie „Gast-Netzwerke“?
Reduzieren der Internetzugriffe „auf das Wesentliche“	Müssen Ihre Server (alle) mit dem Internet kommunizieren? Ist die Funktion des jeweiligen Servers mit den erlaubten Verbindungen der Maschine abgeglichen? Wurde in Ihrem Unternehmen die Notwendigkeit eines Proxyservers beachtet? (Im Zweifelsfall: ein Proxyserver ist fast Immer sinnvoll...)
Ausbildung / Wissenstand der Mitarbeiter	Wie ist der (IT-)Ausbildungsstand Ihrer Mitarbeiter? Existieren Vorgaben für das Verhalten im Fehlerfall? Wurden mit der IT-Abteilung bzw dem IT-Verantwortlichen Vorgaben für ein Krisenmanagements erarbeitet?

Quellen: https://www.bsi.bund.de/DE/IT-Sicherheitsvorfall/Unternehmen/unternehmen_node.html
https://www.wirtschaftsschutz.info/DE/Veroeffentlichungen/Wirtschaftsgrundschutz/Bausteine/Sicherheitsvorfallmanagement.pdf

Über die PROXESS GmbH

PROXESS ist Softwarehersteller und Lösungsanbieter für Dokumentenmanagement, Belegerkennung und Workflow - und dies seit über 25 Jahren. So verstehen wir uns auch als Pioniere des Dokumentenmanagements. Unser Credo dabei ist: Solide und gleichzeitig zukunftsweisende, innovative Softwarelösungen entwickeln und anbieten.

Mit unserem Hauptsitz in Rietheim-Weilheim und Niederlassungen in Leipzig, Rengsdorf (Westerwald) und im schweizerischen Thayngen finden Sie uns schnell und nah im gesamten deutschsprachigen Raum. Über unser Partnernetzwerk werden unsere Lösungen in 26 Ländern eingesetzt.

Wir unterstützen Unternehmen bei der Gestaltung ihrer digitalen Dokumentenprozesse von morgen. Dabei begleiten wir unsere Kunden von Anfang an mit Fachkenntnis, Erfahrung und mit unserem ausgeprägten Servicegedanken.

PROXESS® **PROXESS GmbH**
www.proxess.de