HOPE IS NOT A PLAN 2.0 UPDATE 2024

Erkenntnisse und Ableitungen aus Cyber-Attacken, denen die steirische Industrie ausgesetzt war.

INHALT

Im vorliegenden Papier liegt der Fokus auf **Ransomware** (bzw. am Ende auf **CEO-Frauds**) da es hier einzelne massive Attacken in der Steiermark gab. Es gibt aber zahlreiche weitere mögliche Angriffsarten, u.a.:

- **Spyware**, die das Ziel hat, Nutzeraktivitäten oder sonstige Daten auszuspähen;
- **Sonstige Schadsoftware** – z.B. Viren, Würmer oder Trojaner;
- **Manuelles Hacking**, d.h. Manipulation von Hard- und Software ohne Nutzung spezieller Schadsoftware;
- **Denial of Service** ((D)DoS-) Attacken, die auf eine Überlastung von Web- oder E-Mail-Servern zielen
- **Defacing-Attacken**, die das Ziel haben, unbefugt Webinhalte des Unternehmens zu verändern;
- **Phishing**, bei welchem Mitarbeiter mit echt aussehenden E-Mails oder Webseiten getäuscht werden, um an Zugangsdaten etc. zu kommen.

CYBERCRIME – EINE SEHR REALE BEDROHUNG

Die Konfrontation mit Cyber-Angriffen in verschiedensten Ausprägungen ist mittlerweile zur **realen und regelmäßigen Bedrohung von produzierenden Unternehmen** in Österreich und der Steiermark geworden. Die Zahl der Angriffe ist in den vergangenen Monaten, auch bedingt durch verschiedene geopolitische Strömungen, nochmals stark angestiegen. Im Jahr 2022 wurden laut Cybercrime Report 2022 des Österreichischen Bundeskriminalamtes (BKA) 60.195 Fälle angezeigt, nach 46.179 im Jahr davor und 35.915 in 2020. Im Jahr 2016, waren es „nur" 13.103. Allein von 2019 weg hat sich die Zahl mehr als verdoppelt.

Die Aufklärungsquote lag zuletzt bei 33,9 Prozent und ist in den letzten fünf Jahren stabil geblieben. Hinzu kommt, dass nach wie vor davon auszugehen ist, dass die Dunkelziffer, also die Zahl nicht registrierter Fälle, sehr hoch ist. Schon im Cybercrime Report aus 2020 heißt es: „Viele Betroffene scheuen die Anzeige bei der nächsten Polizeidienststelle, teils aus Scham, Angst vor Reputationsverlust oder weil angenommen wird, dass der Fall ohnehin nicht verfolgt werden könnte."

Die Industriellenvereinigung Steiermark (IV) hat in Zusammenarbeit mit der Technischen Universität Graz und in Kooperation mit dem Zentrum für sichere Informationstechnologie-Austria (A-SIT) im Jahr 2021 ein Projekt initiiert, das zum Ziel hatte, die wesentlichen **Erkenntnisse und Lehren aus den Cyber-Attacken der jüngeren Vergangenheit** in der Steiermark zu erfassen und innerhalb der steirischen Industrie zur Verfügung zu stellen. Zwei Jahre später führten IV und A-SIT neuerlich Gespräche mit jenen Betrieben, die an der Erhebung im Jahr 2021 beteiligt waren. Unsere Gesprächspartner waren dabei die **Geschäftsleitungen und IT-Verantwortlichen** steirischer **Industriebetriebe aus fünf verschiedenen Branchen.**

Die zentralen Ableitungen der im Jahr 2021 durchgeführten und im November 2023 wiederholten Gespräche haben wir in dieser Broschüre zusammengefasst. Auf Basis der konkreten Rückmeldungen der betroffenen Betriebe sollen so das **Bewusstsein für die Bedrohung** gestärkt und zugleich **konkrete Leitlinien für Handlungen zur Prävention** und mögliche **Handlungsszenarien in der konkreten Angriffssituation** aufgezeigt werden.

Die Inhalte richten sich dabei in erster Linie an Unternehmensleitungen, die sich dem Thema Cybersecurity annähern oder ihre aktuellen Maßnahmen vergleichen wollen und dabei von den Erfahrungen anderer steirischer Industriebetriebe profitieren wollen.

In einem **Dialog mit der Landespolizeidirektion Steiermark** war es uns ein Anliegen, Positionen, Möglichkeiten und Rolle der Polizei im Falle von Cyber-Attacken zu beleuchten. Gemeinsames Ziel ist es, die Zusammenarbeit der Strafermittlungsbehörden mit betroffenen Unternehmen und privaten IT-Dienstleistern im Sinne der geschädigten Organisationen zu professionalisieren. Bei Cybercrime handelt es sich um organisierte Kriminalität, die nicht von einer Polizeibehörde isoliert bearbeitet und aufgeklärt werden kann. Cybercrime-Ermittlungen beruhen daher auf enger internationaler Zusammenarbeit, die von Institutionen wie Europol, Interpol, sowie staatlichen Ermittlungsbehörden in mehreren Ländern gemeinsam geführt werden. Je mehr Fälle zur Anzeige gebracht werden, desto umfangreicher können Spuren von den Strafverfolgungsbehörden ermittelt werden. Umso wichtiger ist es uns, Chancen der Zusammenarbeit mit der Polizei aufzuzeigen.

Aufgrund der eingangs angeführten Entwicklungen haben sich die Unternehmen in den vergangenen Jahren intensiv mit den möglichen Bedrohungs-Szenarien beschäftigt und dabei insbesondere entsprechende **Kompetenzen aufgebaut** sowie ihre **IT-Security Ressourcen verstärkt.** Der Aufbau von Ressourcen gestaltet sich jedoch häufig schwierig - nicht selten ist die mangelnde Verfügbarkeit von Fachkräften die Ursache dafür.

Unternehmen berichten, dass die Bedeutung des Themas "IT-Sicherheit" in der Organisation in den vergangenen Monaten weiter in den Vordergrund gerückt ist. Informationssicherheit ist so wichtig, dass es sich um keine Empfehlungen, sondern um **klare Vorgaben** handelt. Dafür ist es nötig, dass der Vorstand voll und

ganz hinter dem Thema und den einzelnen Maßnahmen steht. Das IT-Budget ist in den meisten Betrieben in den vergangenen zwei Jahren stärker als der Umsatz gewachsen.

Eine zentrale Botschaft der betroffenen Unternehmen ist es, die Halbwertszeit des erhöhten Bewusstseins nach einem Vorfall bei den Mitarbeiterinnen und Mitarbeitern nicht zu überschätzen. Vielmehr ist eine **permanente Präsenz des Themas** wichtig. Dies sicherzustellen ist eine der wichtigsten **Aufgaben der Führungskräfte.**

Problematisch ist auch das vermehrte Auftreten von **Identitätsdiebstahl**, der zunehmend auch für Unternehmen ein ernstzunehmendes Risiko wird. Cyberkriminelle nutzen gerne den guten Ruf von Firmen, um daraus Profit zu schlagen. Hierbei ist allerdings besonders schwierig, solche Diebstähle einzuschränken und im konkreten Fall dagegen aktiv werden zu können.
In den Gesprächen und im vorliegenden Papier haben wir uns auf **Ransomware** und damit in Zusammenhang stehende Cyber-Attacken fokussiert. Im Zuge des Projektes wurden uns schon im Jahr 2021 und auch 2023 von unseren Gesprächspartnern auch eine große Zahl an **„CEO Frauds“** geschildert. Aus diesem Grund haben wir uns entschlossen, dieser Art von Angriff neuerlich ein eigenes Kapitel zu widmen.

Wir hoffen, mit dieser Publikation einen Beitrag im Sinne der IT-Sicherheit der steirischen Industrie leisten zu können und bedanken uns bei allen an diesem Projekt teilnehmenden Betrieben sowie der Landespolizeidirektion Steiermark.

Mag. Gernot Pagger
Industriellenvereinigung Steiermark

DI Karlheinz Rink
Industriellenvereinigung Steiermark

DI Herbert Leitold
A-SIT, Zentrum für sichere Informationstechnologie – Austria

DIE FRAGE IST NICHT OB, SONDERN WANN.

Die Einfallstore in das jeweilige betroffene Unternehmenssystem sind sehr unterschiedlich. Der Öffner des Tores ist in den allermeisten Fällen jedoch am **„Faktor Mensch“** festzumachen.

Es scheint **keine allgemein gültigen konkreten Hinweise** auf eine bevorstehende Attacke zu geben. Einige unserer Gesprächspartner vermuten, dass durch mediale Berichterstattung, insbesondere über herausragende wirtschaftliche Erfolge und Entwicklungen, die Aufmerksamkeit potenzieller Angreifer auf das jeweilige Unternehmen gelenkt wurde. Es werden offenbar gezielt Unternehmen gesucht, die Lösegeldforderungen auch erfüllen können.

Die Angriffe sind meist **hochprofessionell, arbeitsteilig organisiert und langfristig vorbereitet**. Die Angreifer befinden sich üblicherweise über einen längeren Zeitraum (von rund zwei Wochen bis hin zu mehreren Monaten) im System und spionieren es unbemerkt aus. Erfahrungen von vor zwei Jahren haben gezeigt, dass es oft selbst rückblickend schwer möglich gewesen wäre, die Anwesenheit der Angreifer zu bemerken. Neue IT-Lösungen oder externe Dienstleistungen wie **Security Operations Center (SOC)** machen mittlerweile ein solches Vorgehen besser erkennbar und können ein Ausbreiten unter Umständen gänzlich verhindern.

Die konkrete, für das Unternehmen sichtbare Durchführung der Attacke erfolgt zumeist zu denkbar ungünstigsten Zeitpunkten. Insbesondere wurden die Nacht von Freitag auf Samstag, Fenster- und Feiertage oder ganz spezifisch auch der Urlaubsantritt des IT-Verantwortlichen genannt.

Oftmals bleibt unklar, wie der Zugang zum System geschaffen wurde. Konkrete Handlungen von Mitarbeitern dürften aber in den meisten Fällen ein wesentliches Einfallstor in die Unternehmen darstellen. So wurde uns unter anderem berichtet, dass die Installation eines Backdoors für die Angreifer durch ein geöffnetes (privates) E-Mail auf der Plattform eines Mailanbieters zustande kam.

Häufig erfolgt der Angriff über das **Einfallstor** eines **Phishing Mails**. Bei einer Attacke ist es beispielsweise dazu gekommen, dass ein Mail, das vor langer Zeit vom Benutzer verschickt worden ist, zwei Jahre später vermeintlich vom Empfänger dieser Mails beantwortet wurde. Dieser Antwort war dann bspw. ein pdf-File angehängt, im pdf-File war ein Bild eingefügt, das insgesamt mit einem Link hinterlegt war. Der Link vernetzte mit einer beliebigen internationalen Website, über die dann weitere Scripts geladen wurden (ohne Download Prompt, vom User völlig unbemerkt), die anschließend im Hintergrund starteten. Welche Websites für eine solche Vorgangsweise verwendet werden, variiert. Es handelt sich um an sich seriöse, aber ebene kompromittierte Websites.

Zum technischen Verständnis eines solchen Angriffs empfehlen wir den Artikel „New QBot email attacks use PDF and WSF combo to install malware“ von Lawrence Abrams:
https://www.bleepingcomputer.com/news/security/new-qbot-email-attacks-use-pdf-and-wsf-combo-to-install-malware/

Vermehrt sind auch besonders perfide Phishing-Mails im Umlauf. Unternehmen werden von ihnen bekannten Lieferanten kontaktiert, die behaupten eine Information per **QR-Code** zu übermitteln. Tatsächlich führt das Scannen des QR-Codes auf eine Phishing-Seite. Kriminelle versuchen dabei, an die Zugangsdaten für das Microsoft-Konto der Mitarbeiter zu kommen. QR-Codes haben aus Sicht der Angreifer den Vorteil, dass sie meist über Handys abgerufen werden und so Sicherheitsstandards der angegriffenen Unternehmen umgangen werden.

Dies ist nur ein Beispiel, das erfolgreiches Phishing beschreibt. Der **Werkzeugkasten der Angreifer ist größer und gut bestückt.** Breit gestreute Emails verweisen auf Gewinnspiele, ahmen Nachrichten von Versandhandel oder Zustelldiensten nach, oder geben sich als Behörde aus. Spezifisch an ein konkretes Unternehmen gerichtet beziehen sie sich auf unternehmensinterne Strukturen oder geben sich als Kunden oder Lieferanten aus. Dabei sind die Nachrichten mittlerweile in perfektem Deutsch verfasst, „sperrige“ Sprache, die vor einiger Zeit noch häufiges Indiz für Phishing war, verschwindet KI-gestützt zusehends.

Sind die Angreifer erfolgreich in das System eingedrungen, **arbeiten sie sich unbemerkt im System hoch**, weiten die Privilegien auf lokalen Maschinen aus, bis sie Accounts mit entsprechenden Domain Admin-Rechten gehackt haben. So wird ein Angriff auf das Netzwerk möglich. Weitere Admin User werden am Domain Controller angelegt. Alle Passwörter aller anderen Admins werden überschrieben. Der Basisserver für andere virtuelle Server wird verschlüsselt – damit sind auch alle anderen virtuellen Server verschlüsselt. Danach werden Daten unbemerkt abgesaugt und Daten auf allen Maschinen, die erreichbar sind, verschlüsselt. So sind sehr rasch zahlreiche Clients betroffen.

Die **Verschlüsselung** erfolgt meist **abrupt, enorm schnell und umfassend**. Es werden nicht nur die operativ unmittelbar verwendeten Datensätze, sondern auch alle erreichbaren Sicherungen im System überschrieben oder gelöscht.

Der gesamte Netzwerk Traffic wird abgefangen und Daten werden gestohlen. Die Server werden verschlüsselt, alle PCs, die zu einem gewissen Zeitpunkt im Netz waren, sind verschlüsselt. Daten werden wahllos abgezogen. Um Unternehmen zu erpressen, werden dann **personenbezogene Daten** (Arbeitsverträge, Reisepässe, …) gesucht und **mit deren Veröffentlichung gedroht**. Hohe Strafzahlungen aufgrund der Verletzung der Datenschutzgrundverordnung (DSGVO) werden von den Erpressern in den Raum gestellt. In einzelnen Fällen wurden wenige einzelne Systeme unverschlüsselt gelassen, womit die Angreifer Kommunikationsmöglichkeiten offenhalten.

In der konkreten Attacke gilt es zunächst, sich einen Überblick zu verschaffen: **Wer ist betroffen? Was und wie viel ist betroffen?** Primäres Ziel der Erpresser ist es, das Unternehmen lahmzulegen (löschen bzw. verschlüsseln von Produktionsdaten) und sensible Daten (Personal, Unternehmen, Preiskalkulationen …) als Druckmittel (Veröffentlichung im „Darknet“) zu besitzen.

Die Angriffe erfolgen teilweise **arbeitsteilig**. Das heißt, dass einzelne Gruppen in das Unternehmen eindringen, andere den tatsächlichen Angriff durchführen und wieder andere die Erpressung und Verhandlung abwickeln. Der jeweils getätigte Schritt der Attacke wird in solchen Fällen dann von einem Angreifer zum anderen als Art spezialisierte Dienstleistung weiterverkauft.

Die **Kontaktaufnahmen durch die Angreifer** erfolgen auf verschiedenen Wegen, meist jedoch hochprofessionell. So werden bspw. die Anweisungen der Erpresser in jedem Ordner auf den noch verfügbaren Laufwerken abgelegt oder es werden automatisiert die Forderungen an allen Druckern und an jedem Stand-

ort des betroffenen Unternehmens ausgedruckt. Die **Verhandlungen** werden teilweise über das **„Darknet“** organisiert und geführt. Teilweise wird die Kontaktaufnahme von den Erpressern über Geschäftsfall-Nummern organisiert, die den Eindruck erwecken, dass die Erpresser Mühe haben, die große Zahl an gleichzeitig durchgeführten Attacken im Überblick zu behalten.

Die Erpresser nennen ihre Forderung und eine Deadline für die Zahlung. Sie bieten bei Bezahlung die Entschlüsselung und die Rückgabe aller personenbezogenen Daten. Sie werden häufig als höflich beschrieben, die gerne den Angriff als Dienstleistung darstellen, mit deren Hilfe das betroffene Unternehmen auf Schwachstellen im IT-System aufmerksam gemacht wurde. In seltenen Fällen wurde aber auch von aggressivem Verhalten und massiven (persönlichen) Drohungen berichtet.

Erfolgt eine Zahlung durch das betroffene Unternehmen, besteht **keine Garantie**, aber eine gewisse Wahrscheinlichkeit, dass die Angreifer ihre Zusagen einhalten. Es muss aber bewusst sein, dass die Angreifer für die Entschlüsselung der Daten eventuell nochmals in das System des Unternehmens einsteigen müssen. Hinzu kommt, dass niemals eine Sicherheit geboten werden kann, dass keine „Backdoors“ im Netz verbleiben. Der tatsächliche Ransomware-Angriff ist zumeist die Folge dessen, dass mehrere Angreifergruppen in äußerst privilegierte Accounts eingedrungen sind. Jede einzelne Gruppe hatte hier die Möglichkeit (und ein unbestreitbares wirtschaftliches Interesse), unbemerkbare Backdoors im System zu hinterlassen und es kann darüber hinaus nicht sichergestellt werden, dass alle am Angriff Beteiligten durch eine allfällige Lösegeldzahlung bedient wurden. Der entstandene Schaden eines erfolgreichen Angriffs ist in jedem Fall enorm.

Firmen, die Lösegeld bezahlt haben, berichten davon, dass Angreifer aus momentaner Sicht eher Wort halten, es gibt aber keine Sicherheiten. Letztlich kauft man sich demnach nur Zeit – **ein neuer Aufbau der IT-Umgebung ist unerlässlich.**

Hinzu kommt, dass die Produktion für eine beträchtliche Zeitspanne zum Stillstand kommt oder zumindest schwer beeinträchtigt ist. In den analysierten Vorfällen konnten Core-Services von betroffenen Unternehmen zwar binnen ein bis zwei Wochen wiederhergestellt werden, die Wiederherstellung der vollständigen Funktionsfähigkeit der Systeme dauerte im Regelfall jedoch deutlich länger.

Es wird mehrheitlich empfohlen, den Kontakt zu den Erpressern nicht abzubrechen – auch wenn man die Entscheidung getroffen haben sollte, nicht zu bezahlen.

„UNSERE DATEN SIND UNSER GOLD“

Eine absolute Sicherheit vor Angriffen aus dem Netz gibt es nicht. Ziel kann und muss es aber sein, die Barrieren und den Aufwand für Angreifer möglichst hoch zu halten und gleichzeitig auf den Eventualfall gut vorbereitet zu sein, um dann den Schaden möglichst gering zu halten. Unternehmen haben mehrheitlich retrospektiv berichtet, dass sie die eigene IT-Sicherheit überschätzt haben.

PRÄVENTION

„Es gibt keine 100%ige Sicherheit. Die Frage ist lediglich, wie stelle ich mich auf, dass der Schaden im Fall der Fälle limitiert ist“, meint ein CEO eines angegriffenen Unternehmens in einem zur Erstellung dieser Broschüre geführten Gespräch.

Präventive Maßnahmen sollen sowohl ein Eindringen von Angreifern und damit den Schadenseintritt überhaupt bestmöglich verhindern, aber eben auch bei einem Vorfall die Auswirkungen begrenzen. Hier sind sowohl technische als auch organisatorische Vorkehrungen, insbesondere die **Bewusstseinsbildung bei Mitarbeiterinnen und Mitarbeitern,** wesentlich.

Alle befragten Unternehmen nehmen hierfür die Expertise von professionellen Anbietern für die Absicherung ihrer IT in Anspruch. Dies vor allem aufgrund der größeren Expertise, wegen regelmäßiger Updates der Tools und weil sich in Summe damit auch das Kosten/Nutzen-Verhältnis besser darstellt.

TECHNIK

In den befragten und betroffenen Unternehmen waren die IT-Organisation und IT-Sicherheit durchaus auf gutem Niveau. Es waren ganzheitliche Ansätze wie IT-Service-Management oder Informationssicherheitsmanagement nach üblichen Standards (oder an solche angelehnt) vorhanden, nach Unternehmen und Branche bzw. Betriebsgröße jedoch in unterschiedlicher Tiefe und Reife.

Auch in der technischen Prävention zählen die bereits angeführten zwei Aspekte: Einerseits gilt es, durch präventive Maßnahmen ein Eindringen möglichst zu erschweren und andererseits, in Vorbereitung einer möglicherweise unvermeidbaren Kompromittierung, durch Steigerung der Resilienz den möglichen Schaden gering zu halten.

Ein **ganzheitlicher Ansatz** ist in der Informationssicherheit immer wesentlich. Es verdienen im speziellen Fall des Schutzes vor Ransomware die häufigen Einfallstore E-Mail und kompromittierte Webseiten, zusammen mit der folgenden Privilegien-Erhöhung des Angreifers bis zum Domänenadministrator, besondere Aufmerksamkeit. Hiermit geht die besondere Beachtung der Endgeräte und das Rechtekonzept (meist im Active Directory) einher.

An den Endgeräten gilt es, die Angriffsfläche zu minimieren. **Endgeräteschutz mittels Virenscanner o. ä.** ist hier zwar Grundlage. Da Angreifer nachgeladene Schadsoftware aktuell halten und damit die Erkennung durch Endgeräteschutz auch oft umgehen können, ist dies **alleine** aber **nicht ausreichend**. Die Angriffsfläche kann vor allem auch dadurch reduziert werden, dass an Endgeräten üblicherweise nicht benötigte Elemente deaktiviert werden. Beispiele hierfür sind PowerShell, Batch-Skripte oder Office-Makros. Zu berücksichtigen sind im Netzwerk auch alte Protokolle, wie NetBios over TCP/IP, auf die als Fallback zurückgegriffen wird, wenn ein System sonst nicht aufgelöst werden kann.

Betroffene Unternehmen berichten auch, dass sie seit den Angriffen die **Mehrfaktorauthentifizierung** breiter und möglichst durchgängig ausrollen. Dies sichert insbesondere auch Remote-Zugänge, die nicht zuletzt durch Home-Office häufiger wurden, und erschwert Angreifern immens, diese als Eindringpunkte zu verwenden.

Die **Aktualisierung der Betriebssysteme und der Software**, sowohl der Endgeräte als auch der Server, in regelmäßigen, kurzen Perioden ist eine wesentliche Vorsorge. Dies vermindert sowohl initiale Einfallstore an den Endgeräten als auch eventuelle Schwachstellen, die ein Angreifer später zur Privilegien-Erhöhung zu Administratorrechten ausnutzen würde.

Für die rechtzeitige Erkennung eines Angriffes haben die befragten Unternehmen vor zwei Jahren überlegt, Ereignismanagement (sog. SIEM – Security Information and Event Management) und aktives Monitoring (über sog.

Security Operations Center SOC) einzuführen. Eine Herausforderung im Einrichten eines SOC ist die dazu spezifisch notwendige Kompetenz, die auch 24/7 verfügbar sein müsste, um effektiv zu sein. Dies ist intern personell kaum erreichbar und bedarf darauf spezialisierter Dienstleister. Zwei Jahren nach den ersten Interviews hatten die dann wieder befragten Unternehmen allesamt SOC beauftragt und damit die **Erkennung von Angriffen** an solche **Dienstleister übertragen**.

In allen Maßnahmen ist für Unternehmen mit **mehreren, internationalen Standorten** deren Gesamtheit zu betrachten. Dies gilt auch im **Zusammenspiel mit Zulieferern oder Dienstleistern**. So erfolgte bei einem befragten Unternehmen der Eintrittspunkt des Angreifers über die Kompromittierung seines ERP-Providers. Das Durchreichen eigener Sicherheitsstandards an Auftragnehmer oder deren IT-Sicherheitsniveau zum Teil der Auswahlentscheidung zu machen, etwa über Zertifizierungen oder Zusicherung der Einhaltung von Standards, ist überlegenswert. Herausfordernd kann dies in internationalen Projekt- und Kundenbeziehungen sein, wobei das Niveau sehr unterschiedlich sein kann. Hier sollte die Notwendigkeit einer vertieften IT-Integration gegen den notwendigen Schutz der eigenen Systeme abgewogen werden. Einige befragte Unternehmen berichten vom erfolgreichen Einsatz eines mehrstufigen Integrationsmodells in Abhängigkeit vom Security-Niveau des Partnernetzes.

Das bei allen befragten Unternehmen wesentlichste technische Element zur Schadensbegrenzung war das **Backup-Konzept**. Eine vollständige und funktionierende Sicherungskopie wurde von einigen Unternehmen als Rettung vor dem Totalverlust beschrieben, während bei anderen das Fehlen einer solchen die Wiederherstellung der Systeme schmerzhaft verzögerte. Allerdings ist dies natürlich auch Angreifern bewusst. Hier muss erneut betont werden, dass es sich bei modernen Ransomware-Attacken nicht um einen „Computervirus“ im klassischen Sinn handelt, der mehr oder weniger ungesteuert Systeme befällt. Vielmals sind die Angreifer nach der Initialinfektion eine intelligente Präsenz, die sich ähnlich wie ein System-Administrator im Netz bewegt.

In Folge sind Online-Backups, die von einem Nutzer mit Administratorrechten gelöscht oder überschrieben werden können, von äußerst beschränktem Nutzen. Bei betroffenen Unternehmen haben sich stufenweise Verfahren mit Online-, aber insbesondere Offline- (Band im Tresor) oder WORM- (Write Once, Read Many) Medien, bewährt. Weiters ist eine **regelmäßige Überprüfung der Backup-Aktivität** unabdinglich, da im Zuge einer langwährenden Angreiferpräsenz sonst die Backup-Prozesse auch möglicherweise für mehrere Monate deaktiviert gehalten werden, bevor der tatsächliche Akt der Verschlüsselung gesetzt wird. Ein Rückspielen nach einem Angriff benötigt aber auch die Information, seit wann Systeme beeinträchtigt waren, um nicht in einen bereits kompromittierten Status wiederherzustellen.

Weitere präventive Maßnahmen zur Reduktion des möglichen Schadens zielen auf eine **Minimierung der vom Angreifer erreichbaren Systeme** ab. Hier ist zu beachten, dass die Angreifer nicht nur auf Speicher der Betriebs- und Produktionsdaten abzielen. Bei einem betroffenen Unternehmen wurden sämtliche virtuelle Maschinen verschlüsselt. Hiermit waren alle Server und damit alle Services, etwa auch die Telefonanlage, betroffen.

Ein Ansatz ist die **Segmentierung**, um Bereiche voneinander abzuschotten. Befragte Unternehmen berichten davon, nach den Angriffen ihre Netzwerksegmentierung zu erweitern. Bei einigen bis hin zu Mikrosegmentierung, mit der die Rechenzentren hochgranular (etwa einzelne virtuelle Maschinen) in Sicherheitszonen getrennt werden.

Einige betroffene Unternehmen berichten, seit einem Angriff das **Rechtesystem mit Domain Administratoren im Active Directory** zu überdenken. Während es für die Systemadministration effizient ist, alle Systeme eines Unternehmens mittels eines einzelnen oder einiger weniger Accounts verwalten zu können, gilt dasselbe natürlich auch für einen Angreifer. Diese hochgradig privilegierten Accounts stellen einen „single point of failure“ dar, der die schnelle Kompromittierung großer Teile des Netzwerks erlaubt. Dazu gibt es durchaus Empfehlungen, zumindest kritische Systeme nur unter lokalen und dabei unterschiedlichen Administratoren-Accounts zu betreiben.

Ein **Einbinden privater Geräte ins Netzwerk,** insbe-

sondere von Smartphones, soll nur über ein entsprechendes **Bring Your Own Device (BYOD)** Konzept erfolgen. Dies beginnt mit dem Abruf der dienstlichen Emails, um sonst bestehende lokale Schutzmechanismen der Dienstgeräte nicht über unbekannte Situation von privaten Geräten zu konterkarieren.

Nach erfolgreichen Angriffen haben Unternehmen die **IT Sicherheit** kontinuierlich gestärkt. Dies wird als kein einmaliges und abgeschlossenes Projekt, sondern als **kontinuierlicher Prozess** beschrieben. Vor allem wurde in vielen Betrieben Multifaktor-Authentifizierung lückenlos umgesetzt. Die meisten Unternehmen lassen **Penetrationstest** von professionellen Partnern sowohl extern aus dem Internet als auch aus dem internen Netz durchführen. Letzteres dient der Erkennung interner Schwächen, um im Fall der Kompromittierung eines Systems die Verbreitung im internen Netz zu erschweren.

Informations-Assets werden definiert und einem laufenden Screening unterzogen, sodass bei ungewöhnlichem Zugriff Alarme erfolgen können. Betriebe kommunizieren dabei auch aktiv mit befreundeten Partnern wie Kunden und Lieferanten, falls sich Vermutungen eines Angriffs ergeben.

Eine aktive Vorbereitung bedarf der Kenntnis der Assets, welche offline zu sichern sind und über welchen Zeitraum dies zu erfolgen hat. Die Kenntnis um eine Sicherung oder ein Krisenplan reichen hier für effizientes Reagieren im Krisenfall nicht aus. Die Wirksamkeit muss sichergestellt sein, dazu sind **regelmäßige Übungen** sinnvoll. Je realitätsnäher diese durchgeführt werden, desto eher werden Lücken in den Plänen aufgezeigt. Ebenso ist das **Aufarbeiten von Vorfällen** sinnvoll, um entsprechende Lehren ziehen zu können.

Zusammenfassend sind die zu Ransomware **wesentlichen Empfehlungen** und von befragten Unternehmen getroffenen technischen Maßnahmen:

- Unnötige Features auf Endgeräten und Servern deaktivieren (Powershell, Makros, Skripts)
- Häufige Updates aller Endgeräte und Server
- Immer auch Offline-Backups zu halten (Band im Tresor)
- Mehrfaktor-Authentifizierung, insbesondere bei Remote-Zugriffen von außerhalb
- Granulares Rechtekonzept (keine globalen Admins für alle Systeme im Active Directory)
- Segmentierung des Netzwerkes in stärker voneinander abgeschottete Zonen
- Analyse des Netzwerkverkehrs, professionelle SOC zur Überwachung des Netzes
- Regelmäßige Penetrationstests, interne Security Audits, sowie Krisenübungen

Befragte Unternehmen lehnen sich im **Informationssicherheitsmanagement** an die ISO/IEC 270xx Serie oder den IT-Grundschutzkatalog des deutschen Bundesamts für Sicherheit in der Informationstechnik an, im IT-Service-Management ist ITIL gängig. Ein weiterer einschlägiger Standard ist ISO 22301 zum Management der Betriebskontinuität.

Immer mehr Unternehmen führen **Darknet-Screenings** durch oder haben diese beauftragt, in denen regelmäßig über das eigene Unternehmen recherchiert wird. Jedenfalls ist es in diesem Zusammenhang essenziell, für potenzielle Angreifer keine Angriffsflächen anzubieten.

Nach einer Cyber-Attacke erhöhen alle betroffenen Unternehmen ihr IT-Sicherheitsbudget massiv. Es gibt keinen Indikator (bspw. bezogen auf den Umsatz), der als Benchmark für eine möglichst IT-sichere Unternehmenssituation herangezogen werden kann. In immer mehr Betrieben werden **Investitionen in die IT-Sicherheit zum unumgänglichen Faktor und als fixer Bestandteil des notwendigen Investitionsprogramms** betrachtet. Aus dem Bewusstsein für den hohen Stellenwert der Datenverfügbarkeit und -sicherheit für die weitere Unternehmensentwicklung, sind uns Investitionsanteile von bis zu 50% des Gesamtinvestitionsvolumens genannt worden. Einzelne Betriebe haben berichtet, dass das IT-Investitionsprogramm der kommenden 3 Jahre binnen 2 Monaten nach dem erfolgten Angriff umgesetzt wurde.

Konkret notwendige Investitionsschwerpunkte (Hardware, Software …) lassen sich allgemeingültig nicht ausmachen. Für das professionelle **Auslagern von Services** sprechen jedoch auch bei unternehmens- und branchenübergreifender Betrachtung drei Aspekte:

1. Fehlende interne Ressourcen
2. Fehlendes internes Know-how (Qualifikation)
3. Benchmarking durch externe Experten mit anderen Unternehmen wird möglich, „Betriebsblindheit“ wird verhindert

MENSCH UND ORGANISATION

Der vielfach zitierte Satz „Es ist nicht die Frage, ob, sondern nur die Frage, wann…“ wurde in den Gesprächen mehrmals bestätigt. Umso wichtiger ist es, möglichst sicherzustellen, dass man als Organisation im Falle eines Angriffs in eine geplante Situation eintreten kann.

Entscheidend ist es für die Vorbereitung auch, dass im Fall eines Angriffes jene **externen Partner**, die in die IT-Sicherheit eingebunden sind, unmittelbar **verfügbar** sind. Eine Empfehlung lautete daher, dass man die Telefonnummer der jeweiligen Experten kennen sollte, um keine Zeit zu verlieren, falls die Attacke am Wochenende oder in der Nacht stattfindet.

Firmeneigene Sicherheitsstandards sollten allen Kunden und Lieferanten abverlangt werden, bei denen Schnittstellen zum IT-System des Unternehmens bestehen. Über **„Permission Management“** sind Kunden leichter „IT-sicher“ zu integrieren als über reine Bewusstseinsbildung für das Thema Cyber-Security. Dies gilt auch für Fragen der Fernwartung durch Hersteller von Anlagen, die im Unternehmen im Einsatz sind. Die Dauer eines Prozesses, der dies sicherstellen soll, darf nicht unterschätzt werden (mehrere Monate).

„Unsere Daten, unser Gold“, daher sollte nicht auf Anforderungen von Kunden oder Versicherungen gewartet werden, sondern im eigenen Interesse der Datensicherheit hochgehalten werden.

Insbesondere die **Schulung von Mitarbeiterinnen und Mitarbeitern** wurde in den vergangenen Monaten intensiviert. Dazu gehören bspw. quartalweise Trainings oder auch Phishing-Kampagnen, um das firmeninterne Bewusstsein zu schärfen. So werden beispielsweise Einladungen zu Firmenfeiern verschickt, zu denen man sich mit begrenzter Teilnahmemöglichkeit und unter einer knappen zeitlichen Vorgabe (um den Druck zu erhöhen) unter einem bestimmten Link anmelden

kann. Die Ergebnisse solcher Kampagnen werden anschließend mit der Belegschaft breit diskutiert.

Die Betriebe stellen erfreulicherweise fest, dass ihre Schulungsmaßnahmen wirken. Die Zahl der geöffneten Links nimmt ab – es können aber auch in bereits von Cyber Attacken betroffenen Betrieben solche Einfallstore nicht zu 100 Prozent verhindert werden, so dass immer auch ein Restrisiko bleibt (es wurde in den Gesprächen von „Klick-Raten“ im Bereich von einigen bis über zehn Prozent berichtet).

Lösungen für Schulungen und Kampagnen können über fertige Produkte zugekauft werden und standortspezifisch ausgestaltet werden. Diese Tools ermöglichen von der Serienaussendung bis hin zu einer individuellen Analyse, wer Links oder Dokumente geöffnet hat und ggf. auch, wer vertrauliche (Anmelde-) Daten eingegeben hat.

Neuen Mitarbeiterinnen und Mitarbeitern fallen Ungereimtheiten tendenziell eher nicht auf. Sie sind **besonders anfällig** und sollten in Schulungen entsprechend speziell adressiert werden. Ebenso macht es Sinn, dass die Schulungssoftware in den für das Unternehmen relevanten Sprachen betrieben werden kann.

IT-Sicherheit und die Rolle jedes einzelnen Mitarbeiters wird in unterschiedlichen Medien für Mitarbeiter und Kunden kommuniziert. Beteiligungen am Unternehmenserfolg (Prämien) werden mancherorts davon abhängig gemacht, ob der entsprechende Mitarbeiter an IT-Security Schulungen teilgenommen hat. Erfolgskontrollen von Schulungen werden u.a. auch durch die personenbezogene Dokumentation der Korrelation zwischen der Teilnahme an Schulung und erfolglosen Phishing-Versuchen durchgeführt. Auf Basis dieser Analysen können auch sehr gut allenfalls weitere notwendige weitere Maßnahmen und Schulungen definiert werden.

Wesentliche Unternehmensleitsätze, die in den Gesprächen genannt wurden, sind:

- Security betrifft jeden Mitarbeiter und jede Mitarbeiterin an allen Standorten.
- Security ist kein isoliertes Thema der IT-Abteilung.
- Jeder ist Security.
- Führungskräfte sind wichtige Vorbilder.

Im gesamten Projektmanagement sollen Datenschutz und Security als fester Bestandteil integriert werden. Das regelmäßige Durchspielen von „Fake-Angriffen" (mit externen Dienstleistern möglich) wird angeraten und bringt wesentliche Erkenntnisse über den tatsächlichen Sicherheitslevel der Organisation und der jeweiligen Person.

Ein möglicher, von einem Unternehmen genannter Ansatz wäre, dass wenn ein Mitarbeiter eine Website aufrufen will, welche im System noch nicht freigeschaltet ist, diese zunächst „white-gelistet", also von der IT-Abteilung geprüft und freigegeben werden muss. An dieser Stelle sei darauf aufmerksam gemacht, dass die Ausgestaltung von IT-Sicherheitsmaßnahmen immer eine **Gratwanderung zwischen Sicherheit und Usability** darstellt. Es besteht das Risiko, dass Mitarbeiter Umwege suchen, wenn die subjektiv wahrgenommenen Einschränkungen zu groß sind (Trade Off). Alle Sicherheitsmaßnahmen stellen für Mitarbeiter zusätzlichen Aufwand und Unannehmlichkeiten dar. Der Versuch von Umgehungen ist Realität und sollte in allen Strategien und Lösungen mitgedacht werden.

Bei Unternehmen mit mehreren Standorten muss bewusst sein: Die kleinste Einheit mit auch nur einem Mitarbeiter kann die Sicherheit des Gesamtunternehmens gefährden. Es sind **daher gleiche Spielregeln für alle Standorte** festzulegen und einzuhalten.

Einzelne Unternehmen haben ein **Krisenstab-System** etabliert, in dem ein Cyber-Angriff (neben Arbeitsunfällen, Hochwasser, COVID-19, Black-Out …) eines der Szenarien ist, auf das man sich vorbereitet hat. Ziel ist es, im Fall der Fälle bessere Entscheidungen treffen zu können. Es sind Führungsgebiete, Befugnisse und Zuständigkeiten definiert und entsprechende Krisenräume vorbereitet. Entscheidungen werden in Krisensituationen klar strukturiert und hierarchisch getroffen. Das Agieren im Krisenstab wird regelmäßig trainiert. Der Prozess, einen solchen Krisenstab einzurichten, ist überaus aufwändig, bewährt sich aber in der entsprechenden Situation jedenfalls.

Für das Vorbereiten konkreter Dokumente und Wordings spricht, dass so die Reaktionsgeschwindigkeit in der Krise erhöht werden kann. Dagegen spricht die Individualität einer Krise, für die man ein Framework, aber keine vorgefertigten Lösungen bereithalten kann. Unternehmen haben in den vergangenen Monaten vermehrt eigene **Information Security Officer** installiert. Sie und ihre Teams haben die Verantwortung für die Erstellung und Kontrolle der Einhaltung von IT-Security Richtlinien, wie auch für entsprechende Schulungen der Mitarbeiterinnen und Mitarbeiter.

Die Mitarbeiter-Systeme (wie PCs) werden mit aktuellem Client-Schutz ausgestattet, was als Grundausstattung Virenscanner und lokale Firewalls umfasst, zunehmend auch Lösungen wie Mail-Firewalls und Öffnen der Anhänge in Sandboxes, bis zu Zero-Trust Prinzipien, wo einem Endgerät grundsätzlich nicht mehr vertraut wird, sondern Identität und Integrität immer erst überprüft wird. Ist die Entscheidung für neue IT-Lösungen im Unternehmen getroffen, kann es dazu kommen, dass **lange Lieferzeiten** deren Umsetzung hinauszögern und so die Verwundbarkeit von Unternehmen länger gegeben ist.

Es wird empfohlen, alle im Fall eines erfolgreichen Angriffs nötigen externe Dienstleister (IT-Unternehmen bis Anwaltskanzleien) rechtzeitig und laufend einzubinden. Im Falle eines Angriffs sind gut informierte und eingebundene Partner an der Seite des Unternehmens äußerst wertvoll.

WÄHREND DES ANGRIFFS

TECHNIK

Die Entscheidung, ob ein Vorfall forensisch untersucht werden soll, um die mögliche Quelle des Angriffs bzw. die Vorgehensweise der Angreifer zu ermitteln, **ist früh zu treffen.** Dies kann aus Haftungsfragen oder für den Versicherungsschutz notwendig sein. Bei befragten Unternehmen hat auch die Versicherung hierauf spezialisierte Dienstleister vermittelt. Die frühe Entscheidung ist notwendig, um bei der Wiederherstellung nicht die für die Analyse notwendigen Daten wie Logs zu zerstören. Für ein paralleles Neuaufsetzen der IT bei gleichzeitigem Behalten der Altsysteme zu Zwecken der Forensik ist oftmals eine unerwartete Menge an Speicherplatz notwendig. Dies sollte in der Frühphase der Wiederherstellung bedacht werden.

Hinsichtlich der **Trennung aller Systeme vom Internet ist abzuwägen**, ob die Kommunikation mit den Angreifern für eine Bezahloption noch offen gehalten werden soll oder ohnehin davon ausgegangen wird, dass selbst wieder neu aufgesetzt wird. Bei letzterem Vorgehen empfiehlt sich das vorerst vollständige Trennen vom Internet, um Angreifern damit keinen direkten Zugriff mehr zu geben. Ein befragtes Unternehmen hat es dabei als vorteilhaft gesehen, nur eine Internetanbindung gehabt zu haben und so das Trennen rasch durchführen zu können. Für das Aufsetzen benötigte Netzverbindungen können dann in isolierten, neu aufgesetzten Netzbereichen erfolgen.

Wird nicht komplett vom Internet getrennt, sollte ein Aufruf an Mitarbeiterinnen und Mitarbeiter bzw. auch an Standorte erfolgen, vorerst nicht an das Netzwerk zu verbinden.

Verschlüsselte Daten müssen aus Haftungsgründen aufbehalten werden. Dies kann die Speicherkapazität des Unternehmens an seine Grenzen bringen und macht unter Umständen den raschen Ankauf von Speicherplatz nötig.

KOMMUNIKATION UND ORGANISATION

Kommunikation Extern

Die Art und Weise, wie in der konkreten Angriffs-Situation nach außen kommuniziert wird, hängt sowohl vom Umfang des Angriffs als auch von möglichen Schäden in Folge unterlassener Information ab. Grundsätzlich gibt es bei keinem Unternehmen eine fertig vorbereitete Liste, wer wie informiert werden sollte. Vielmehr sind **klare Zuständigkeiten und entsprechende Prozesse definiert**, um rasch und einfach diesbezügliche Entscheidungen treffen zu können.

Kunden und Lieferanten kommunizieren nach Einschätzung unserer Gesprächspartner im Fall von Attacken oft zu wenig. **Offene Kommunikation stellt die einzige Chance dar, dass Partner zeitgerecht reagieren können.** Eine als vertrauenswürdig eingestufte Quelle sollte sofort entsprechend behandelt werden können, wenn sie das nicht mehr ist.

Aktive Kommunikation wird als **Gebot der Fairness** von verlässlichen Partnern gesehen. Auch wenn dies kurzfristig mit Nachteilen verbunden sein kann, handelt es sich aus Sicht der betroffenen Betriebe um die einzige faire und seriöse Vorgangsweise. Und um die einzige Vorgangsweise, die nicht mittel- und langfristig zu massiven Reputationsverlusten führt.

Lieferanten und Geschäftspartner sollen auch aus Gründen des Datenschutzes und allfällig betroffener persönlicher Daten aktiv informiert werden. Von den betroffenen Unternehmen wurde uns vor zwei Jahren eine weite Bandbreite an Reaktionen der informierten Betriebe berichtet, die von einem Kappen (bzw. Sperren) des Zuganges bis hin zu angebotenen Kooperationen bei der Behebung der Probleme an der jeweiligen Schnittstelle reichten. Zuletzt haben wir praktisch ausnahmslos die Rückmeldung erhalten, dass Geschäftspartner und Kunden für eine offene Kommunikation dankbar sind und meist sehr viel Verständnis für die Situation zeigen.

Die **Kommunikation in Richtung Öffentlichkeit und Medien** wurde in den betroffenen Unternehmen **sehr unterschiedlich gesehen und umgesetzt.** Als Argument gegen eine aktive Kommunikationsarbeit wurde angeführt, dass die Erpresser eventuell ein besseres Bild über die Situation des Unternehmens und die Auswirkungen des Angriffs erhalten. Dies kann insbesondere auch die Verhandlungsposition mit den Erpressern negativ beeinflussen. Die Kommunikation nach außen sollte ausschließlich durch eine zentrale Stelle (Geschäftsführung, Corporate Communications …) gestaltet werden.

Es können interimistische Websites vorbereitet und eingerichtet werden, auf denen im Falle eines erfolgreichen Angriffs offen kommuniziert wird und Notfall-Telefonkontakte für Kunden und Lieferanten genannt werden.

Auch hinsichtlich der **Datenschutzmeldungen an Behörden** empfiehlt sich offene Kommunikation. Alle personenbezogenen Daten von deren Diebstahl man weiß, sollten bei den Behörden gemeldet werden. Strafzahlungen konnten so in der Praxis sogar gänzlich vermieden werden.

In der Kommunikation nach außen ist eine rechtliche Beratung jedenfalls sehr zu empfehlen, um Wordings und damit in Zusammenhang stehende allfällige Haftungen berücksichtigen zu können. So wurde beispielsweise in den Interviews berichtet, dass von der Formulierung „Wir entschuldigen uns …" gegenüber Geschäftspartnern bewusst abgesehen wurde.

Kommunikation Intern

Die Kommunikation sollte zentral und top-down organisiert erfolgen. Tägliche Updates an Mitarbeiter und Partner sollten so gestaltet werden, dass sie immer vollumfängliche Informationen bieten (nicht nur die Neuigkeiten der letzten Stunden), um das Gesamtbild und den Kontext der jeweiligen Information sicherzustellen. **Vom Diebstahl persönlicher Daten betroffene Mitarbeiterinnen und Mitarbeiter** sollten aktiv und direkt kontaktiert und informiert werden.

Während des Angriffs ist es ratsam, regelmäßig (täglich) klar strukturierte **Arbeitssitzungen** eines idealerweise im Vorfeld definierten **Krisenteams** abzuhalten, um **Arbeitspakete und Kommunikationsregeln** festzulegen.

Diese Sitzungen zu dokumentieren kann auch hilfreich gegenüber Versicherungen und Behörden sein – jedenfalls auch, um mit zeitlichem Abstand die gesetzten Schritte zu analysieren und Erkenntnisse für die Zukunft abzuleiten („Manöverkritik").

In vielen Unternehmen wurde ein Notfalls-Kommunikationsmedium für den Krisenfall vorbereitet, etwa Alarmierungssoftware und Krisenmanagementsysteme. Es wird als essenziell eingestuft, dass insbesondere der Erstkontakt (inkl. Einberufung eines Krisenstabs) über alternative Kanäle über (meist cloudbasierte) Notfalls-Tools möglich ist, die losgelöst von Mail und Telefonie funktionieren.

Wird in dieser Phase die Suche nach der „schuldigen Person" in den Fokus genommen, behindert dies meist die Lösung der tatsächlichen Krisensituation.

Es wird empfohlen, eine klare Sprachregelung zu vereinbaren, die auf die gewählte Strategie hinsichtlich der Kommunikation nach außen Rücksicht nimmt (z.B.: keine Kommentare an Externe, „Technische Probleme" oder „Cyber-Attacke", „An der Lösung wird gearbeitet").

Die Kontaktaufnahme zu Mitarbeitern (auch zur IT-Abteilung!) wurde in manchen Fällen dadurch erschwert, dass keine Kontaktdaten mehr verfügbar waren. Es empfiehlt sich daher, eine **Kopie möglichst aller (privater) Mailadressen und Telefonnummern aller Mitarbeiterinnen und Mitarbeiter in Papierform** anzulegen bzw. auch ein Mindestmaß an weiteren wichtigen Informationen (z.B. Wiederanlaufpläne o. ä.) in gleicher Form zu dokumentieren.

Die **Kommunikation über Bypässe** (SMS, WhatsApp oder Signal und über dort vorab zu ursprünglich anderem Zweck eingerichtete Gruppen) hat in vielen Fällen funktioniert und in der Situation das Austauschen von Informationen erleichtert.

Insbesondere während des Angriffs, aber auch in der daran anschließenden Phase der Schadensbeseitigung bzw. der entsprechenden Adaptierung des IT-Systems, ist es wichtig, in der **internen Kommunikation** die dafür zuständigen Mitarbeiter vor unnötigen Anfragen abzuschirmen.

Kommunikation mit Erpressern

Im Kontakt zu Erpressern soll darauf abgezielt werden, den Effekt des Datendiebstahls möglichst gering zu halten.

Es scheint zwei grundsätzliche **Szenarien der Erpressung** zu geben, von denen berichtet wurde: Gezielte Angriffe auf einzelne Unternehmen mit enormer Lösegeldforderung und Angriffe auf mehrere Unternehmen

(bspw. über ein ERP-System, das diese Unternehmen anwenden), verbunden mit vergleichsweise geringer Lösegeldforderung. Der Rahmen für die Kommunikation mit den Erpressern ist in diesen beiden Fällen durchaus unterschiedlich. **Die Höhe der Lösegeldforderung** im Fall einer gezielten Attacke liegt erfahrungsgemäß zwischen 0,75 und 1,5 Prozent des Jahresumsatzes des Unternehmens. Für die Verhandlungen wurde von den betroffenen Unternehmen eine Reduktion von bis zu 50% als realistisch angegeben.

Der Druck, der auf Eigentümer und/oder Geschäftsführung während den Verhandlungen lastet, wird als enorm beschrieben.

Es empfiehlt sich, grundlegend und vorab im Unternehmen festzuhalten, wie im Falle eines Angriffs vorgegangen wird. Ein eventuelles kategorisches Ausschließen von Zahlung sollte bereits vor einer Attacke entschieden und allen Führungskräften bewusst sein. Auch sollte geklärt sein, wer den Kontakt zu den Erpressern hält. Die **Verhandlungen mit den Erpressern** sollten über einen Chat auf einem separaten Laptop geführt werden. Um jede Möglichkeit einer Spionage zu unterbinden, sollte sich dieser Laptop in einem separaten, versperrten Raum befinden, in dem keine sonstigen Gespräche stattfinden. Zudem sollte die Kamera des Laptops abgeklebt werden.

Der Namen des Verhandlers des Unternehmens sollte möglichst nicht genannt werden. Jedenfalls sollte die Verhandlungsführung nicht eine exponierte Person des Unternehmens übernehmen (Geschäftsführer, Eigentümer), da Fälle bekannt sind, in denen diese Personen auch persönlich bedroht wurden (Informationen auf Basis von Internet-Recherchen, Facebook, etc.). Private Details zu den verhandelnden Personen sollten im Idealfall im Internet nicht auffindbar sein.

Bei der Verhandlung mit den Erpressern ist zu berücksichtigen, welche Daten die Angreifer generiert haben und welche Folgen eine tatsächliche Veröffentlichung im „Darknet" hätte. Nicht zuletzt deshalb ist es auch wichtig, nach Möglichkeit herauszufinden, über welche Daten die Erpresser tatsächlich verfügen. Die Angreifer schicken üblicherweise auf Nachfrage beispielhaft konkrete Dateien, um zu beweisen, dass sie diese tatsächlich besitzen.

Bei den Gesprächen mit den Erpressern gilt, wie es ein Unternehmensvertreter auf den Punkt gebracht hat: „Jeder Tag, den man länger durchhält, reduziert die Lösegeldforderung und stärkt zugleich die eigene Position." Für die Verhandlung mit den Angreifern werden am Markt bzw. konkret von den Versicherern Spezialisten angeboten, die auf Basis ihrer umfassenden Erfahrung die Erpresser einzuschätzen versuchen und eine optimierte Verhandlungsstrategie wählen.

Bei den Verhandlungen ist zu bedenken, dass auch das Entschlüsseln von allenfalls wieder freigegebenen Daten Zeit braucht. Bei allfälliger Fortführung der Produktion (wenn auch nur in geringem Ausmaß) wird die Datenlücke zwischen Status quo zum Zeitpunkt des Angriffs und aktuellem Stand laufend größer. Es ist abzuwägen, inwieweit ohnehin bzw. ab welchem Zeitpunkt ein völliger Neustart der Datenbasis nötig ist.

Art der Lösegeldabwicklung: Eine häufig auftretende Frage ist, **ob Unternehmen vorsorglich höhere Summen in Bitcoins bereithalten sollen?** Zwar lässt sich dazu keine allgemein gültige Antwort geben (abhängig von zeitlichem Druck oder auch der Qualität der Backups), Experten raten aber eher davon ab. Zum einen scheint es schwierig bis unmöglich, entsprechend hohe Summen bereitzuhalten. Zum anderen ist im konkreten Bedarfsfall die Beschaffung von Kryptowährungen mittlerweile sehr einfach möglich. Außerdem wurde uns berichtet, dass zusehends auch alternative Kryptowährungen (wie z.B. Ethereum) zur Abwicklung von den Erpressern vorgeschlagen beziehungsweise eingefordert werden. Zudem gilt es zu beachten, dass in manchen Ländern das Bezahlen des Lösegelds eine Straftat darstellen kann (weil damit eine kriminelle Vereinigung unterstützt wird).

Organisation

Während einer Attacke ist es schwierig, sich Gedanken über die beste Reaktion zu machen. **Rechtzeitig erstellte Reaktionspläne und Checklisten** oder auch

etablierte Krisenteams helfen bei der Begrenzung des Schadens bzw. einer möglichst strukturierten Vorgehensweise. Die genaue Vorgehensweise im Krisenfall hängt vom jeweiligen Unternehmen ab. Generell haben jedoch alle Gesprächspartner regelmäßige (tägliche) klar strukturierte Arbeitssitzungen in idealerweise im Vorfeld definierten Krisenteams als wesentlichen Ansatzpunkt genannt, um eindeutige Arbeitspakete und Kommunikationsregeln festzulegen.

Wesentlich ist es auch, die im Falle eines Angriffes verfügbaren Ressourcen bestmöglich zu nützen und die unmittelbar **mit der Behebung der Krise befassten Mitarbeiterinnen und Mitarbeiter zu entlasten**, indem ihnen beispielsweise entsprechend abgegrenzte Arbeitsbereiche zur Verfügung stehen bzw. ihnen regelmäßig ausreichende Pausen bzw. Ruhephasen ermöglicht werden.

Betroffene Unternehmen berichten auch, dass die extreme Arbeitslast über mehrere Wochen oft schleichende **mentale Effekte auf die IT-Belegschaft** hat. Ein betroffener Abteilungsleiter hat hier den Vergleich mit einem Marathonlauf getroffen, bei dem eine gute Einteilung der Kraftreserven erforderlich ist. Nach Abschluss der Initialtriage ist auf entsprechende Pausen und Rasttage zu achten, insbesondere auch auf Führungsniveau.

Eine jedenfalls notwendige **Prioritätensetzung** (Hochfahren der Systeme - Standorte, Produktion, Linien, Verwaltungsbereiche, Vertrieb …) muss festgelegt werden und soll offen und aktiv kommuniziert werden. Welche Assets werden gebraucht? In welcher Reihenfolge? Eine solche Priorisierung wird in den Unternehmen unterschiedlich sein. Sehr stark zu empfehlen ist, dass diese schon vor einem Ereignis im Zuge der Krisenvorsorge mit simulierter Annahme eines Komplettausfalls erfolgt. Die **Voraus-Priorisierung** ist enorm wichtig, da beim vollständigen Ausfall jeder Bereich eines Unternehmens das eigene Problem als subjektiv wichtig einschätzt. Hier unter Druck die Reihenfolge der Schritte zu entscheiden, ist ohne strukturierte Vorausplanung für Entscheidungsträger und IT-Abteilungen immens belastend.

BEHÖRDEN & VERSICHERUNGEN

Zunächst gilt es, die allfällig zuständige Versicherung zu kontaktieren bzw. muss vom Unternehmen ebenso die Polizei informiert werden. Es kann aber durchaus länger dauern, bis die Tatbestandsaufnahme erfolgt. Eine Meldung des erfolgten Angriffes ist jedoch rechtlich, und vielfach auch versicherungstechnisch, erforderlich.

POLIZEI

Jeder angezeigte Sicherheitsvorfall sollte aus Sicht des Landeskriminalamtes Steiermark forensisch untersucht werden und die zuständige Polizeidienststelle (Landeskriminalamt) und Strafverfolgungsbehörde (Staatsanwaltschaft) so früh als möglich in die Aufarbeitung eingebunden werden. Ermittlungen im Bereich Cybercrime gestalten sich aufgrund des Umstandes, dass die Täter ihre Angriffe meist aus dem Ausland verüben, sehr aufwändig und zeitintensiv.

Der **zeitlichen Komponente** kommt bei den Ermittlungen von Cybercrime-Fällen insofern eine **besondere Brisanz** zu, als dass Täter bei ihren Interventionen auf kompromittierten Datenverarbeitungsgeräten zumeist sehr volatile Spuren hinterlassen. Seien dies Datenartefakte in Arbeitsspeichern (RAM) oder in Zwischenspeichern (Caches), die im Zuge der weiteren Nutzung eines Datenverarbeitungsgerätes sehr leicht vernichtet werden können. Hinterlassen die Täter Spuren in Form von IP-Adressen oder anderen Internetartefakten, die vom betroffenen Gerät aufgezeichnet wurden, so müssen diese Informationen bei den Internetserviceprovidern gesichert (Data Preservation) und danach von der Staatsanwaltschaft im Wege eines förmlichen Rechtshilfeersuchens (MLAT) für weitere Ermittlungen angefordert werden. Die Einholung dieser Informationen ist meist von rechtlich normierten Speicherfristen des jeweiligen Landes, in dem der Provider seinen Firmensitz hat, abhängig und daher äußerst zeitkritisch.

Aus Sicht des Landeskriminalamtes Steiermark ist es verständlich, dass IT-Dienstleister, die mit der Schadensermittlung und der Wiederherstellung kompromittierter Computerinfrastruktur betraut worden sind, einen anderen Fokus auf einen Sicherheitsvorfall legen als Strafverfolgungsbehörden. Dennoch sollten geschädigte Firmen forensische Datensicherungen den Strafverfolgungsbehörden zur Auswertung zur Verfügung stellen, da diese für die Herstellung gerichtsverwertbarer Beweise benötigt werden.

Die Erstellung stringenter Sachbeweise ist vor allem für die Beweisführung vor ausländischen Strafverfolgungsbehörden unbedingt erforderlich, da diese bei geringstem Zweifel selten geneigt sind, weiterführende Ermittlungen oder Kooperationen zu unterstützen.

Die Aufklärung von Straftaten im Deliktsfeld der Cyberkriminalität dient nicht nur der Durchsetzung der privatrechtlichen Schadensersatzansprüche eines Geschädigten, sondern auch der Generalprävention.

Da die Tätergruppen in Kampagnen meist gegen mehrere Opfer vorgehen, ist bei der Klärung eines Deliktes zu erwarten, dass damit auch die Rechte und Ansprüche einer Vielzahl von Opfer gewahrt werden können.

Je mehr Fälle zur Anzeige gebracht werden, desto umfangreicher können Spuren von den Strafverfolgungsbehörden ermittelt werden, was wiederum eine Steigerung der Aufklärungsrate ermöglicht.

WEITERE STELLEN

Prüfen Sie, ob eine **Datenschutzverletzung** gegeben ist, und erstatten Sie ggf. eine Meldung an die **Datenschutzbehörde** und informieren Sie betroffene Personen. Die Datenschutzbehörde muss innerhalb von 72 Stunden informiert werden – eine zeitnahe Reaktion der Behörde ist nicht zwingend zu erwarten.

Es wird empfohlen, sich **parallel anwaltlich beraten** zu lassen, da die rechtlich relevanten Sachverhalte ineinandergreifen. (Strafrecht, Datensicherheit, Versicherungsrecht …) Bei mehreren betroffenen Standorten in unterschiedlichen Ländern ist es ratsam, separat Anwälte vor Ort einzubinden.

Informationen können auch an **CERT.at** gegeben werden, wo Angriffsbilder gesammelt werden und möglicherweise auf dieser Basis hilfreiche Informationen zu erhalten sind.

VERSICHERUNG

Der Schutz durch eine Versicherung gegen Cyber-Attacken ersetzt die Notwendigkeit einer hohen IT-Sicherheit nicht. Vielfach sorgt er aber für diese automatisch mit, da vor Vertragsabschluss den Versicherern zumeist umfassend über das IT-Risiko berichtet werden muss. Die Versicherer starten (häufig unter Einbeziehen externer Dienstleister) einen **Risiko-Dialog**, im Rahmen dessen das Risiko nicht nur evaluiert wird, sondern vielfach auch erste Maßnahmen abgeleitet werden, die es reduzieren.

Versicherungen bieten im Regelfall eine 24/7-Hotline, werden meist unmittelbar nach dem Angriff in alle Schritte und Maßnahmen eingebunden und stellen oder vermitteln Experten.

Die Koordination von konkreten Maßnahmen während der Attacke kann durch die Versicherung erfolgen, die im Regelfall Experten für Forensik bis Verhandlungsführung mit den Erpressern bereitstellt. Es ist grundsätzlich möglich, auch Lösegeldforderungen in den Versicherungsschutz einzubeziehen – hierfür gibt es jedoch klare Vorgaben. Zum Beispiel müssen Versicherungen für Lösegeld separat (nicht im Gesamtpaket) abgeschlossen und ausgewiesen werden und müssen genau auf das wirtschaftliche Risiko des Unternehmens abgestimmt sein. Die erlaubte Laufzeit ist mit einem Jahr limitiert. Zudem darf weder der Versicherer damit werben, noch darf der Versicherte den Abschluss einer solchen Polizze bekannt geben.

Das Einschalten der Polizei (Landespolizeidirektion bzw. s.o.) ist im Regelfall die Voraussetzung für die Wirksamkeit des Versicherungsschutzes.

Für den Versicherungsschutz ist es wichtig, nachweisen zu können, dass Maßnahmen zur Sensibilisierung der Mitarbeiterinnen und Mitarbeiter für die Sicherheitserfordernisse in der IT (Schulungen, Informationen) tatsächlich durchgeführt wurden.

Informationen bzw. Meldungen an die **Datenschutzbehörde** sind über **https://www.dsb.gv.at/download-links/dokumente.html** (dort dann PDF-Formular) möglich.

Wenn Sie durch eine Straftat geschädigt wurden oder konkrete Hinweise auf einen Täter haben, können Sie die **Straftat in jeder Polizeidienststelle bzw. bei der Landespolizeidirektion zur Anzeige bringen.**

Das **Landeskriminalamt Steiermark** verfügt mit seinem Dauerdienst über einen Service, der unter der Rufnummer **059133 60 3333** (oder dem Polizeinotruf) rund um die Uhr verfügbar ist. Den Beamten des Dauerdienstes des Landeskriminalamtes ist es grundsätzlich jederzeit möglich, den Kontakt zu einem der Beamten des Assistenzbereiches IT-Beweissicherung des Landeskriminalamtes Steiermark herzustellen.

Falls Sie Betreiber wesentlicher Dienste oder Anbieter digitaler Dienste im Sinne des **NIS-Gesetzes** sind (Netz- und Informationssystemsicherheitsgesetz – NISG) und/oder freiwillige Meldung über einen Vorfall erstatten wollen, informieren Sie sich hier: **https://nis.cert.at/**

Wenn Sie einen Verdacht auf Internetkriminalität haben und Hilfe oder Informationen benötigen, können Sie sich auch an das **Bundeskriminalamt** wenden: **Meldestelle für Internetkriminalität against-cybercrime@bmi.gv.at**

Haben Sie eine **Versicherung** für derartige Vorfälle, sollten Sie diese umgehend beiziehen.

Gelten für Sie im Falle von IT-Vorfällen **vertragliche Informationspflichten**, beispielsweise gegenüber Auftraggebern, Geschäftspartnern, Auftragnehmern oder Versicherungen, oder vergleichbare Compliance-Regeln?

Weitere mögliche Anlaufstellen

Cybercrime Competence Center - kurz C4
https://bundeskriminalamt.at/306/start.aspx

Computer Emergency Response Team - CERT.at
https://cert.at/de/ueber-uns/

IKT-Sicherheitsportal
(Meldestellen, Ratgeber, News o.Ä.)
www.onlinesicherheit.gv.at

Cybersecurity-Hotline der WKO:
telefonische Erstinformation unter **0800 888 133**

Aktuelle Informationen, Meldepflichten und Kontaktadressen finden sich auch auf der Homepage der Industriellenvereinigung unter **https://www.iv.at/Themen/Klima--Infrastruktur--Transport--Ressourcen--Energie/cybersicherheit/cybersicherheit.html**

Cyber-Kriminelle versuchen auch in der Steiermark regelmäßig, mit CEO Frauds an Geld von Unternehmen zu gelangen, was sich auch in den Interviews bestätigt hat. Die angewandten Methoden sind dabei durchaus sehr unterschiedlich. Erst im Nachhinein konnte nachvollzogen werden, mit welch großem organisatorischen Aufwand und Geschick die Betrüger dabei vorgegangen sind.

Wesentlich ist, dass der Schaden durch CEO Frauds **im Regelfall von der Versicherung nicht gedeckt** wird.

Die Mails der Führungskräfte wurden teilweise über Monate mitgelesen, um über die Art der Kommunikation der Personen untereinander alle Details zu erfahren. Auch der Zeitpunkt, zu dem der Fraud durchgeführt wurde, war auf die ganz spezifische Situation angepasst. So gab es Betriebs-Spionage mittels Telefon-Anrufen, bei denen unterschiedliche Informationen (aus sozialen Netzwerken wie LinkedIn, XING oder Facebook bzw. sonstige allgemein im Internet auffindbare Informationen) genutzt wurden.

Insbesondere auf die mögliche Gefährdung durch die **Weiterleitung von Anrufen** – wenn externe Rufnummern entweder nicht mehr angezeigt werden bzw. als „intern" wahrgenommen werden könnten, wurde hingewiesen. Ebenso wurde in den Gesprächen auf die zunehmenden Gefahren durch Phishing-SMS (z.B. im Versandbereich „Ihr Paket ist …"), die eventuell in Stress-Situationen irrtümlich geöffnet werden, sowie auch auf gefälschte Geschäftsbriefe, in denen beispielsweise angeblich neue Bankverbindungen der Unternehmen genannt werden, aufmerksam gemacht.

In allen Fällen wurde von Seiten der Betrüger höchst professionell agiert und auf die betroffene Person in der jeweiligen Situation auch direkt massiver Druck ausgeübt. Beispielsweise wurde mit einer Kündigung gedroht, wenn nicht sofort gehandelt wird. Plattformen und Webseiten, auf denen die gewünschten Informationen bekanntzugeben sind, sind hochprofessioneller Nachbau und unterscheiden sich auf den ersten Blick kaum von den Originalen.

Wichtig ist es, das **Bewusstsein für typische Angriffsmuster** zu schärfen. So sollten bspw. Mitarbeiterinnen und Mitarbeiter in der Telefonzentrale bzw. am Empfang klar wissen, welche Auskünfte sie geben dürfen und welche nicht (bspw. Dienstreisen).

Eines der befragten Unternehmen ist dazu übergegangen, allgemeine Informationen, die üblicherweise per Mail an alle Mitarbeiter verschickt werden, auch im Intranet zu spiegeln. Es gilt der Grundsatz: Was nicht im Intranet gespiegelt wird, ist ein Fake.

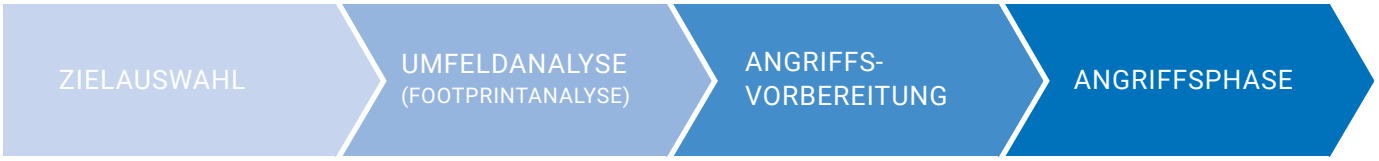
Beim Angriff in Form eines CEO Frauds genutzte Informationen stammen u.a. aus Pressemeldungen, Websites, LinkedIn-Beiträgen, etc. Angreifer sind sehr erfolgreich darin, Bezug zu tatsächlichen Themen im Unternehmen herzustellen und so die Glaubwürdigkeit hochzuhalten.

Änderungen von Bankverbindungen von Mitarbeitern sollten nur nach persönlichen Gegencheck vorgenommen werden.

Hinweise auf mögliche Gefährdungen

Gerade spezielle Umstände, unter denen **Überweisungen** o.Ä. durchgeführt werden sollen, sollten daher verdächtig sein. Ein solches Beispiel wäre ein Anruf der Finanzchefin von einer privaten Handynummer aus dem Urlaub oder eine Mail eines leitenden Mitarbeiters aus dem Home-Office.

Das deutsche Bundesamt für Sicherheit in der Informationstechnik (BSI) hat die Vorgehensweise der Cyber-Kriminellen in vier Phasen unterteilt:



- Liste möglicher Angriffsziele
- Auswertung von Basis-Informationen (z. B. Adresse, Sitz) über Unternehmen

PHASE 2

- Ermittlung der Unternehmensstruktur
- Analyse von Geschäftspartnern
- Aufnahme von Ansprechpartnern
- Auswahl des Angriff-Szenarios (z. B. M&A-Aktivitäten)
- Erste „Insider-" Informationen

- Erste Kontaktaufnahme (telefonisch) zur Verifikation gewonnener Informationen
- Gewinnung aktueller Informationen (z. B. Abwesenheiten)
- Anreicherung der „Insider-" Informationen
- ggf. Beziehungsaufbau
- Festlegung des Angriffszeitraumes
- Festlegung der Höhe des Betrugs

PHASE 4

- Aufbau einer Stress Situation
- Beruhigung der Zielperson durch Insider-Wissen
- Übermittlung der Handlungsanweisung
- ggf. (telefonisches) Nachfassen

Quelle: BSI

Tipps zum Thema CEO Frauds:

- Unternehmen sollten darauf achten, welche Informationen sie über sich bzw. ihre Mitarbeiter wo und an wen preisgeben.
- Die Einführung von Abwesenheitsregelungen und internen Kontrollmechanismen wird empfohlen.
- Im Falle ungewöhnlicher Zahlungsanweisungen sollte immer der Absender genau überprüft werden bzw. der Vorgesetzte oder die Geschäftsleitung kontaktiert werden.
- Außerdem sollten Unternehmen die Mitarbeiterinnen und Mitarbeiter auch über die Gefahr von CEO Frauds informieren.

Quelle: BSI

steiermark.iv.at

IMPRESSUM

IV-Steiermark
Hartenaugasse 17, 8010 Graz
0316/321528
steiermark@iv.at

Für den Inhalt Verantwortlich:
Gernot Pagger, Karlheinz Rink, Jakob Heher

Grafikdesign: Mayrberger Nina
Fotocredits: AdobeStock

Wien, im Februar 2024