HOPE IS NOT A PLAN

Erkenntnisse und Ableitungen aus Cyber-Attacken auf steirische Industriebetriebe

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.

In Kooperation mit: TU Graz A-SIT

Die Internetkriminalität hat in Österreich und damit auch in der Steiermark in den letzten Jahren massiv zugenommen. Im Jahr 2020 wurden laut Cybercrime Report 2020 des Österreichischen Bundeskriminalamtes (BKA) 35.915 Fälle angezeigt. Fünf Jahre zuvor, im Jahr 2016, waren es „nur" 13.103. Allein von 2019 weg ist die Zahl um mehr als 26 Prozent gestiegen. Die Aufklärungsquote lag zuletzt bei 33,4 Prozent, ein Minus von 17,9 Prozent gegenüber dem Jahr zuvor. Die absolute Zahl der aufgeklärten Fälle ist damit zwar gestiegen, hinkt aber der Entwicklung der angezeigten Fälle hinterher.

Zudem vermutet das BKA eine hohe Zahl weiterer, nicht registrierter Fälle: „Die Dunkelziffern im Bereich der Internetkriminalität sind unter Berücksichtigung internationaler Studien besonders hoch. 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", heißt es im Cybercrime Report 2020.

Die Formen der Internetkriminalität sind vielfältig. Industrieunternehmen sind vor allem von erpresserischen Verschlüsselungsangriffen (sog. „Ransomware") betroffen.

Die Industriellenvereinigung Steiermark hat in Zusammenarbeit mit der Technischen Universität Graz und in Kooperation mit dem Zentrum für sichere Informationstechnologie-Austria (A-SIT) ein Projekt initiiert, das zum Ziel hat, die wesentlichen Erkenntnisse und Lehren aus den Cyber-Attacken der jüngeren Vergangenheit zu erfassen und innerhalb der steirischen Industrie zur Verfügung zu stellen. Auf Basis der Rückmeldung von betroffenen Betrieben sollen das Bewusstsein für die Bedrohung gestärkt und konkrete Leitlinien für Handlungen zur Prävention und mögliche Handlungsszenarien in der konkreten Angriffssituation geschildert werden. Basis für die in dieser Broschüre präsentierten Inhalte sind Expertengespräche, die IV-Steiermark, A-SIT und TU Graz mit Geschäftsleitungen und IT-Verantwortlichen steirischer Industriebetriebe aus fünf verschiedenen Branchen geführt haben.

Die wesentlichen Ableitungen der im November 2021 durchgeführten Gespräche finden Sie nachfolgend zusammengefasst. Diese richten sich in erster Linie an Unternehmensleitungen, die sich dem Thema Cybersecurity annähern oder ihre aktuellen Maßnahmen vergleichen wollen und dabei von den die Erfahrungen anderer steirischer Industriebetriebe profitieren wollen.

In den Gesprächen und im vorliegenden Papier haben wir uns auf Ransomware und damit in Zusammenhang stehende Cyber-Attacken fokussiert.

Mit dem Satz "Hope is not a plan" hat einer unserer Gesprächspartner die Situation und die Notwendigkeit der Prävention so treffend zusammengefasst, dass wir uns entschlossen haben, dieses Zitat zum Titel der vorliegenden Publikation zu machen.

Im Zuge dessen wurden uns von unseren Gesprächspartnern allerdings auch eine große Zahl an „CEO Frauds" geschildert. Aus diesem Grund haben wir uns entschlossen, dieser Art von Angriff ein zusätzliches, ursprünglich nicht vorgesehenes 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:

Mag. Gernot **Pagger**
Geschäftsführer IV-Steiermark

Univ.-Prof. Dipl.-Ing. Dr.techn. Stefan **Mangard**
Leiter des Instituts für AIK, TU Graz

Dipl.-Ing. Herbert **Leitold**
Gesamtleiter A-SIT Zentrum für sichere Informationstechnologie – Austria

Dipl.-Ing. Jakob **Heher**
Doktorand am Institut für AIK der TU Graz

Dipl.-Ing. Karlheinz **Rink**
Experte IV-Steiermark

WIE LÄUFT EIN CYBER-ANGRIFF AB? ERFAHRUNGEN AUS DER STEIRISCHEN INDUSTRIE

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.

Die Angriffe sind meist hochprofessionell, arbeitsteilig organisiert und langfristig vorbereitet. Die Angreifer befinden sich üblicherweise über einen längeren Zeitraum (oft mehrere Wochen oder Monate, bei wenig komplexen Systemen allerdings durchaus auch kürzer) im System und spionieren es unbemerkt aus. Erfahrungen zeigen, dass es oft selbst rückblickend schwer möglich gewesen wäre, die Anwesenheit der Angreifer zu bemerken. 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 beispielsweise über die Vermutung berichtet, dass die Installation eines Backdoors für die Angreifer durch ein geöffnetes (privates) E-Mail auf der Plattform eines Mailanbieters zustande kam.

Sind die Angreifer erfolgreich in das System eingedrungen, arbeiten sie sich unbemerkt im System hoch, bis sie Accounts mit entsprechenden Privilegien (Domain Admin im Konzern) gehackt haben.

Die Verschlüsselung der Daten erfolgt meist abrupt, gezielt und umfassend. Es werden nicht nur die operativ unmittelbar verwendeten Datensätze, sondern auch alle erreichbaren Sicherungen im System überschrieben oder gelöscht. Zeitweise werden wenige einzelne Systeme unverschlüsselt gelassen, womit die Angreifer Kommunikationsmöglichkeiten offenhalten.

Zunächst gilt es, 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 Folgen eines möglichen Preisgebens von Firmendaten im „Darknet“ wurden von einem Unternehmen mit dem „Verkauf des Unternehmens ohne die Assets“ beschrieben.

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 Standort 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 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. Andererseits 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. Selbst bei einer Lösegeldzahlung und erfolgreichem Entschlüsseln ist ein vollständiges Neuaufsetzen des Netzwerks unabdingbar. 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 deutlich länger.

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

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

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.

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. Die Wirksamkeit der Aktualisierungsmaßnahmen sollte durch zusätzliche Werkzeuge (z.B. mit Hilfe von Scannern, die Netzwerk-Schwachstellen erkennen) in kurzfristigen, wiederkehrenden Abständen überprüft werden.

Für die rechtzeitige Erkennung eines Angriffes überlegen befragte Unternehmen, Ereignismanagement (sog. SIEM – Security Information and Event Management) und aktives Monitoring (über sog. Security Operations Center SOC) einzuführen. Dies ersetzt jedoch Tests der Effektivität nicht. So hat ein Unternehmen berichtet, dass eine konkrete SIEM-Lösung externe Penetrationstests kaum erkannt hat. Eine weitere 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.

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.

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.

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.

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.

MENSCH UND ORGANISATION

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

Die Awareness-Bildung im Unternehmen kann durch regelmäßige Beiträge in der Mitarbeiterzeitung, im Intranet oder auch in Form von kreativ gestalteten

Aushängen (Comics) forciert werden. Mitarbeiterschulungen sollen laufend und für alle Mitarbeiter abgehalten werden. Kurze Einheiten (E-Learning) mit einer Überprüfung und Dokumentation des Lernfortschritts werden empfohlen. Die Inhalte können von der Verwendung von USB-Sticks bis hin zum Umgang mit Phishing-Mails reichen. Auch das Schildern und Kommunizieren von konkreten Fallbeispielen aus der Realität des Unternehmens hat sich bewährt. Manche Firmen erstellen auch eigene Lernvideos mit eigenen Mitarbeitern, die ihren Kollegen über ihre Erfahrungen berichten.

Besonderes Augenmerk ist auf neu eintretende Mitarbeiter zu richten, die unverzüglich mit den Standards vertraut gemacht werden müssen und die ihr Wissen auch in Form von Überprüfungen unter Beweis stellen sollen.

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 „whitegelistet", 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).

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.

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 eine parallele Neuaufsetzung der IT bei gleichzeitiger Aufbehaltung 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 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 teils 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

Lieferanten und Geschäftspartner sollen aktiv informiert werden – nicht zuletzt aus Gründen des Datenschutzes und allfällig betroffener persönlicher Daten. Sie verhalten sich erfahrungsgemäß äußerst unterschiedlich. Von den betroffenen Unternehmen wurde uns eine weite Bandbreite an Reaktionen berichtet, die von einem Kappen (bzw. Sperren) des Zuganges bis hin zu angebotenen Kooperationen bei der Behebung der Probleme an der jeweiligen Schnittstelle reichen.

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.

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

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“).

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“ statt „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 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.

Kommunikation mit Erpressern

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. Die Verhandlungsführung sollte 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.

Für die Verhandlungsstrategie 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.

Bei den Verhandlungen 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 in Bitcoins 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 oft enorm fordernd, erfolgversprechende Strategien binnen kurzer Frist und unter großem Druck festzulegen. 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.

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?

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.

Kontaktstellen

Die berichteten Erfahrungen haben gezeigt, dass während des Angriffs externe (private) Professionalisten oft mehr und konkretere Hilfestellung anbieten können als öffentliche Stellen.

Meldestelle Polizei
bundeskriminalamt.at/306/start.aspx
bzw. **against-cybercrime@bmi.gv.at**

Die Datenschutzbehörde muss innerhalb von 72 Stunden informiert werden – eine zeitnahe Reaktion der Behörde ist nicht zwingend zu erwarten.

Datenschutzbehörde
www.dsb.gv.at/download-links/dokumente.html
(dort dann PDF-Formular) möglich.

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 Mitarbeiter für die Sicherheitserfordernisse in der IT (Schulungen, Informationen) tatsächlich durchgeführt wurden.

WEITERE LEARNINGS

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:

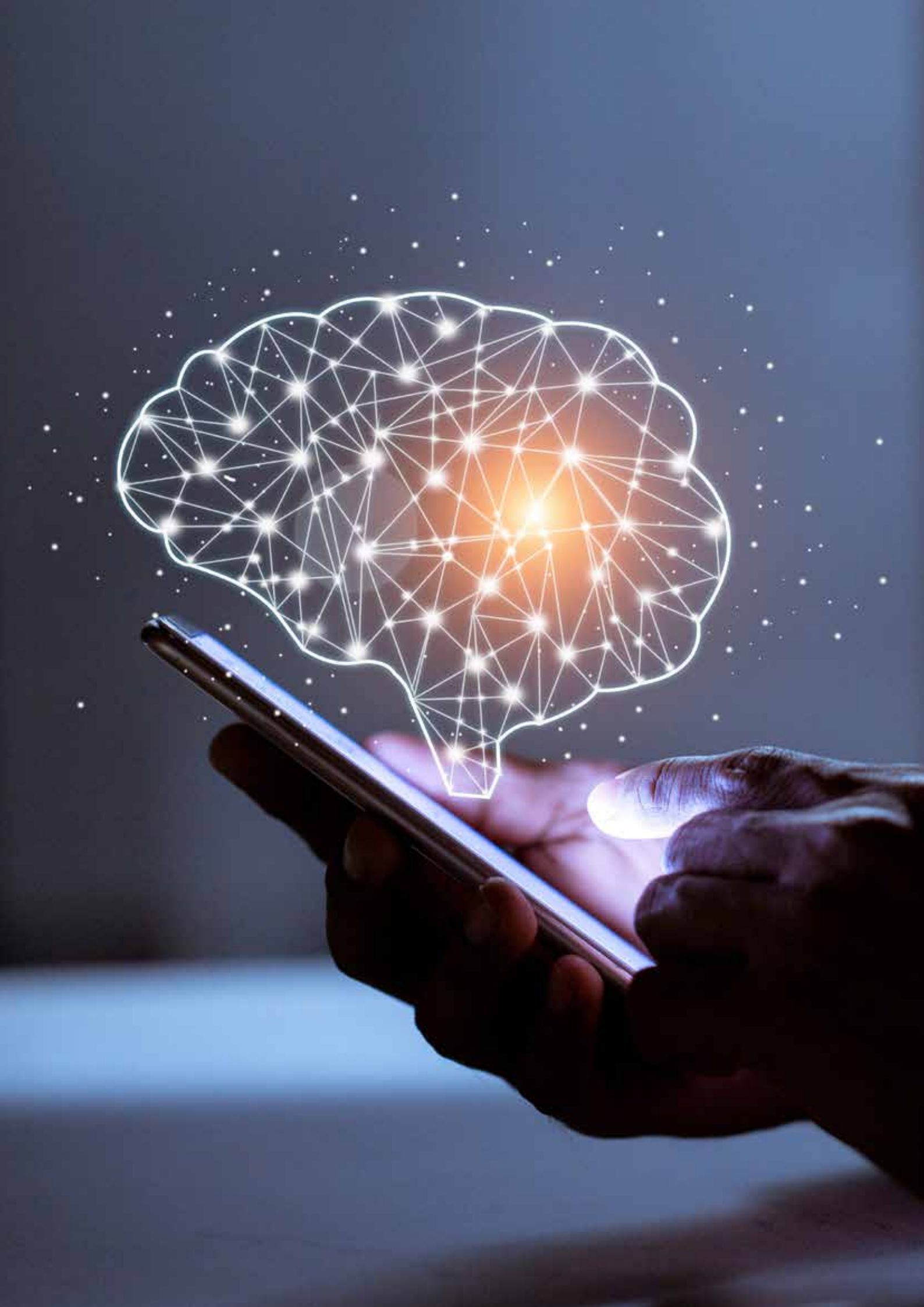
- Fehlende interne Ressourcen
- Fehlendes internes Know-how (Qualifikation)
- Benchmarking durch externe Experten mit anderen Unternehmen wird möglich, „Betriebsblindheit“ wird verhindert

Penetration Tests und fingierte Angriffe durch externe Dienstleister haben auch den Vorteil, dass verschiedene Zugänge und Strategien abgetestet werden können und so blinde Flecken vermieden werden. Externe Berater bzw. Fachexperten sollen möglichst zeitnah ins Boot geholt werden, um sicherzustellen, dass sie das System des Unternehmens im Grundsatz kennen, um im Angriffsfall rasch unterstützen zu können.

Von Analysen, welche Informationen zum eigenen Unternehmen im „Darknet“ ausgetauscht werden, raten die Experten eher ab, da die Recherche selbst für Aufmerksamkeit sorgen könnte.

Eine etwaige Priorisierung, in welcher Reihenfolge welche Services neu aufzusetzen sind, was allenfalls abzuschalten ist oder temporär gelöscht werden kann, 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.

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.



CEO FRAUDS – WENN DER (VERMEINTLICHE) CHEF GELD VERLANGT

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 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.

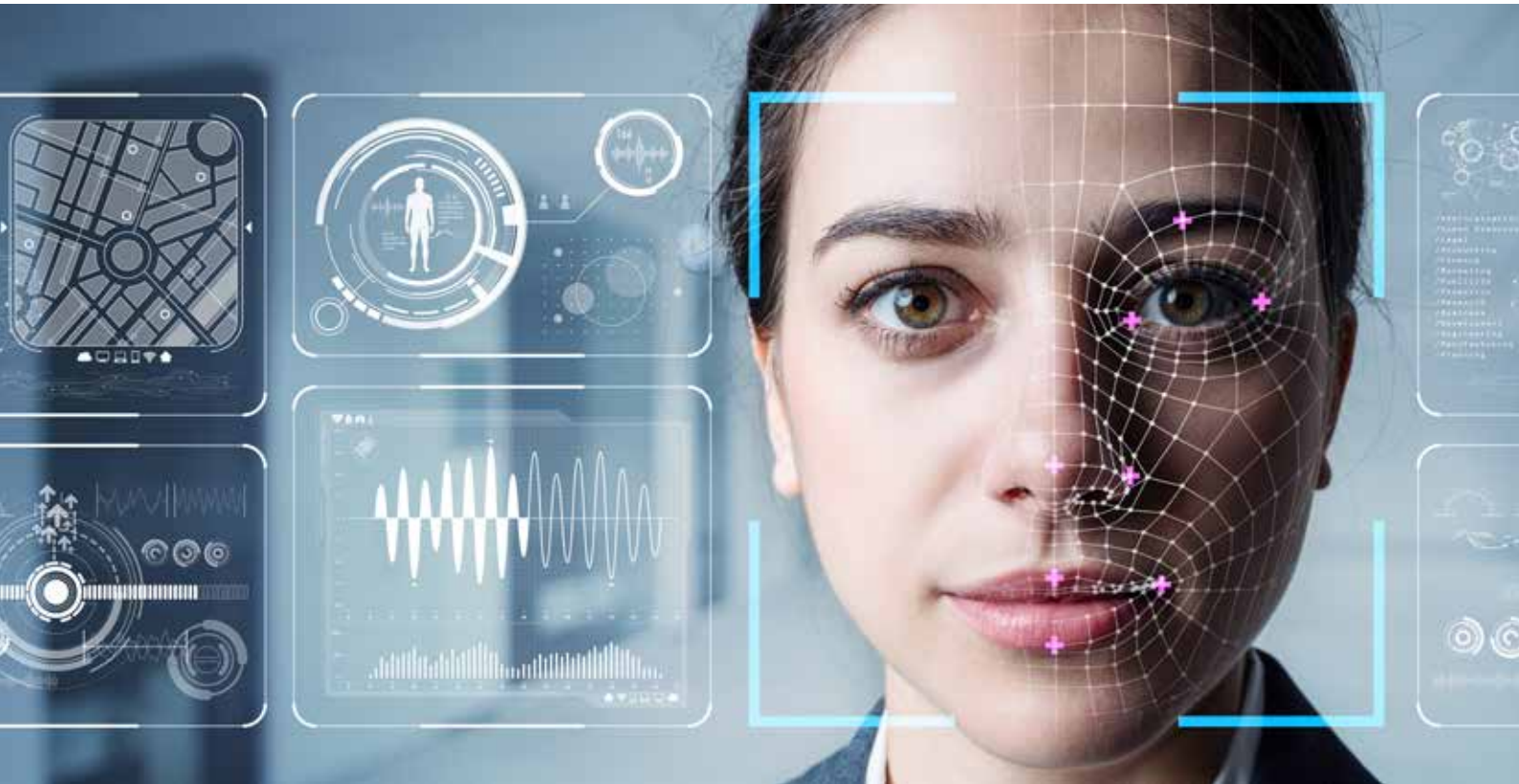
Insbesondere auf die mögliche Gefährdung durch die Weiterleitung von Anrufen – wenn externe Rufnummern entweder nicht mehr angezeigt werden bzw. als „intern" wahrgenommen werden könnten, wurde hingewiesen. Ebenso wurde auf die zunehmenden Gefahren durch Phishing-SMS (z.B. im Versandbereich „Ihr Paket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

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.

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 (siehe Infografik).



- 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 Mitarbeiter auch über die Gefahr von CEO Frauds informieren.

Quelle: BSI

AUF EINEN BLICK: MELDEPFLICHTEN, KONTAKTE UND WEITERE INFORMATIONEN

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

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

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

Aktuelle Informationen, Meldepflichten und Kontaktadressen finden sich auch auf der Homepage der Industriellenvereinigung unter **www.iv.at/cybersicherheit**

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

Anzeige bei der Polizei:

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.

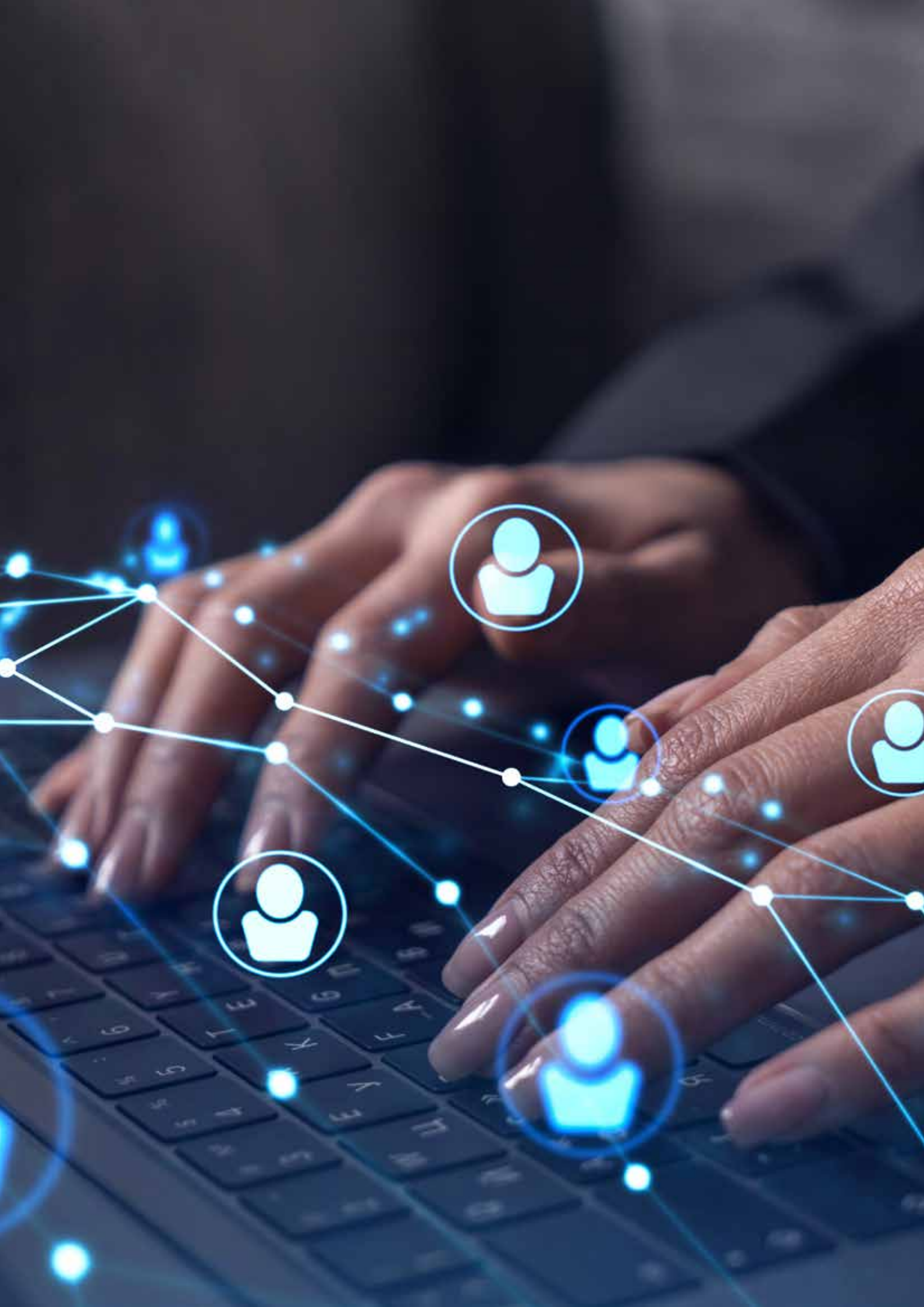
Weitere mögliche Anlaufstellen:

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

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

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

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



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, Herbert Leitold

Grafikdesign: Mayrberger Nina
Fotocredits: AdobeStock

Wien, im Dezember2021