# Cyberkriminelle müssen draußen bleiben

Spätestens mit der Covid-19-Pandemie sind die letzten Unternehmen in der Digitalisierung angekommen. Videokonferenzen, Homeoffice und Ransomware definieren den neuen Arbeitsalltag. Viele Unternehmer*innen sehen sich nicht nur mit diesem Wandel, sondern vor allem auch mit der wachsenden Internetkriminalität überfordert. So gestalten Sie den Einstieg (bzw. Aufbau) Ihrer IT-Security so einfach und frustfrei wie möglich. **THOMAS STEINBRENNER**

Will man das Thema IT-Sicherheit für ein Unternehmen strukturiert angehen, stoßen sogar IT-Security-Expert*innen an ihre Grenzen. Zu komplex und zu umfangreich ist das Thema in den letzten Jahren geworden. Mit all den neuen Erfahrungsberichten, Fachvorträgen, Bedrohungsszenarien, Standards, Vorschriften und Gesetzen, Anlaufstellen und Produkten, die jährlich neu erscheinen, ist es herausfordernd, am Laufenden zu bleiben.

Für Sie als Unternehmer*in haben wir einen kurzen Leitfaden zusammengestellt, an dem Sie sich orientieren und die wichtigen Informationen gut einordnen können. Und keine Angst: Viele Empfehlungen sind organisatorisch und benötigen keine übermäßigen Ausgaben, sondern lediglich ein bisschen Zeit, Aufmerksamkeit und Geduld.

**Das NICE-Framework der NIST** (US-amerikanische Standardisierungsbehörde) identifiziert derzeit 52 (!) Rollen im IT-Sicherheitskontext.

## AM ANFANG WAR DAS INVENTAR

**Wissen Sie, welche IT-Assets Ihr Unternehmen besitzt? Welche davon sind geschäftskritisch?** Sind auch „Testgeräte" und andere scheinbar unwichtige Geräte erfasst? Können Sie rasch und korrekt Auskunft geben, wenn etwas gestohlen oder kompromittiert wurde?

Es kommt nicht nur in großen und komplexen Unternehmen vor, dass der Überblick über die IT verloren geht. Dieser ist aber essenziell, wenn es darum geht, Maßnahmen zu planen und im Anlassfall schnell und entschieden zu handeln. Denn oft sind Testgeräte oder alte Infrastruktur, von der niemand mehr wusste, dass es sie überhaupt noch gibt, ein Einfallstor für Angriffe. Noch schlimmer: Oft ist gar nicht klar, welche Systeme für das Unternehmen geschäftskritisch sind. Und dann fällt genau der eine Server/Switch/Storage aus, den das Logistiksystem benötigt – und ohne Logistiksystem … naja, Sie wissen, was ich meine.

Also: In der Regel genügt eine (Excel-)Liste. Diese kann gleich von der Buchhaltung beim Einkauf und von der IT beim Ausscheiden bzw. bei Änderungen gepflegt werden. Wenn Sie eine eigene Software – wie z.B. baramundi UEM oder Snipe-IT – inklusive Automatisierungsfunktionen zur Verwaltung ihrer „IT-Assets" im Einsatz haben, umso besser.

In der Liste enthalten sein sollten: Typ (Standrechner, Laptop, Drucker, …), Hersteller, Marke & Modell, Seriennummer, Hardware- und Softwareversion, Besitzer*in, Kritikalität sowie Allfälliges wie z.B. die IMEI bei Mobiltelefonen. Die IMEI (International Mobile Station Equipment Identity) ist eine 15-stellige Seriennummer, anhand derer jedes GSM- oder UMTS-Endgerät weltweit eindeutig identifiziert werden kann.

So eine Liste kann schnell und einfach mit Polizei und IT-Security-Dienstleister*innen geteilt werden und auch bei Personalwechsel oder Neubeschaffungen wertvolle Dienste leisten.

## 3-2-1-BACK-UP!

**Sind alle wichtigen Assets in Ihrer Back-up-Strategie enthalten?** Passt die Häufigkeit der Back-ups mit dem RPO (Recovery Point Objective, verkraftbarer Datenverlust) zusammen? Stimmen die Speicherdauern mit den notwendigen (gesetzlichen) Speicherfristen überein? Gibt es einen Notfallplan für die Wiederherstellung der Systeme? Wie schnell fällt auf, wenn ein Back-up fehlschlägt?

Foto: maximalfocus

*Thomas Steinbrenner war nach seinem Studium in Hagenberg über fünf Jahre als IT-Sicherheitsexperte beim BMLVS tätig. Ende 2021 gründete er die Firma Section 8, die KMU bei der Entwicklung und Umsetzung ihrer Cybersicherheitsstrategie unterstützt. www.section8.eu*

Doch Back-up ist nicht gleich Back-up. Auch hier können fatale Fehler passieren. Ein guter Merkspruch ist das „3-2-1-Back-up": Ich brauche drei Back-ups, verteilt auf mindestens zwei Orte und eines davon offline.

Das mit den Standorten ist klar: Wenn Büro und Serverraum abbrennen und alle Magnetbänder und Back-ups gleich mit, hat es wenig gebracht. So kann ein redundantes Back-up an einem zweiten Firmenstandort oder bei einem Dienstleister Gold wert sein.

Ein Offline-Back-up ist ebenso wichtig. Dabei handelt es sich um eine Sicherungskopie, auf die nicht andauernd oder nur schreibend (aber nicht überschreibend!) zugegriffen werden kann. Man könnte auch „revisionssicher" sagen: Sollte ein Fehler oder ein Verschlüsselungstrojaner die immer erreichbaren Back-ups zerstören, sind zumindest die Offline-Back-ups sicher.

## RANSOMWARE

**Wurden Sie schon einmal Opfer eines Cyber-Angriffes** oder hatten Sie bereits einmal Bedenken, dass Sie angegriffen wurden? Welche Gegenmaßnahmen haben Sie getroffen? Was haben Sie daraus gelernt?

Ransomware, auch oft Verschlüsselungstrojaner genannt, sind derzeit wohl bei Weitem die größte und vor allem sichtbarste Bedrohung für Unternehmen. Hier steht man jedoch nicht einfach einem Stück Software gegenüber, sondern hochspezialisierten Gruppen, die wie Firmen strukturiert und geführt werden. In sorgfältiger Handarbeit werden Daten verschlüsselt und alle gefundenen Back-ups vernichtet, um gegen Lösegeldzahlung eine Entschlüsselung anzubieten.

Falls man bezahlt, finanziert man damit nicht nur das Wachstum eines kriminellen Unternehmens, sondern potenziell auch Terrorismus oder die nordkoreanische Rüstungsindustrie (vgl. Lazarus-Gruppe). Die Herausgabe der Daten nach Bezahlung ist damit auch nicht gewährleistet.

Wenn Sie glauben, dass Sie als Unternehmer*in diesem hochspezialisierten organisierten Verbrechen in Preisverhandlungen oder durch unbeholfene Analyseversuche etwas entgegenzusetzen haben, dann ziehe ich meinen Hut vor Ihnen. Alle anderen sollten sich professionelle Hilfe holen – mehr dazu später.

Wer glaubt, dass der Blitz nicht zweimal an derselben Stelle einschlägt, irrt sich ebenso fatal. Wenn man einmal unter Beweis gestellt hat, dass man leichte Beute ist, folgen die nächsten Angriffe in Kürze – denn nur wenige Unternehmen setzen nach einem erfolgreichen Angriff geeignete Gegenmaßnahmen.

**Wegen eines internen Streits wurden 2022** von jener kriminellen Gruppe, die für die Conti-Ransomware verantwortlich war, interne Nachrichten veröffentlicht. Dies gab tiefe Einblicke in die Struktur der einzelnen Abteilungen: Zwischen 60 und 100 Personen sollen im Kernteam und 250 im Umfeld arbeiten.

## SCHWACHSTELLEN

**Verwenden Sie nur aktuelle Betriebssystem- und Softwarestände?** Haben Sie unnötige Systeme und Services ausgeschaltet? Erkennen Sie neue Schwachstellen schnell, rechtzeitig und automatisch? Wissen Sie, welche Maßnahmen Sie ergreifen müssen, wenn kein Patch (Update, das Fehler oder Sicherheitslücken behebt) zur Verfügung steht?

In der Regel nutzen Ransomware-Gruppen über brandaktuelle „Exploits" (Angriffsmethoden, die Schwachstellen ausnutzen) die üppig vorhandenen Schwachstellen. Diese können sich durch veraltete Betriebssysteme und ungepatchte Systeme genauso wie durch Fehlkonfigurationen und alte, verwundbare Protokolle bzw. Services auftun.

Doch was kann man dagegen tun? Seien Sie ein möglichst unattraktives Ziel! Patchen Sie Ihre Infrastruktur rasch und oft. Deaktivieren Sie alte und unnötige Software und Protokolle. Verwenden Sie nur aktuelle Betriebssystemversionen. Verfolgen Sie Nachrichten und Neuigkeiten rund um aktuelle Bedrohungen und Schwachstellen.

Im Idealfall verwenden Sie eine Schwachstellenmanagementsoftware (z.B. tenable, Holm Security VMP), die Sie automatisch vor alten und neuen Schwachstellen warnt und somit wertvolle Zeit spart. Diese erkennt oft nicht nur Software-, sondern auch Konfigurationsschwachstellen, die genauso gefährlich sein können.

**Zwischen der Veröffentlichung von kritischen Patches** und der automatisierten flächendeckenden Ausnutzung der darin gestopften Lücken liegen teilweise nur 15 Minuten.

## VON WOLKEN UND LUFTSCHLÖSSERN

**Verwenden Sie Cloud-Produkte?** Kennen Sie die rechtlichen Rahmenbedingungen der Cloud? Sind die Zuständigkeiten („Shared Responsibility Model") geklärt und dokumentiert?

Viele Unternehmen lagern ihre IT-Infrastruktur in die Cloud aus und hoffen damit, all diesen Problemen zu entgehen. „Das Rechenzentrum, in dem wir sind, ist ISO 27001 zertifiziert", bekommt man manchmal stolz zu hören. Das ist gut, aber die Zutrittskontrollsysteme und internen Prozesse des Rechenzentrums schützen Sie nicht davor, schlechte Passwörter zu wählen, Server falsch zu konfigurieren, kein adäquates Back-up zu haben oder Patches nicht rechtzeitig einzuspielen. Sich auf den Cloudbetreiber auszureden, macht so viel Sinn, wie mit einem defekten Auto und schlechter Fahrweise bei einem Unfall auf den Straßenerhalter zu zeigen: keinen.

Das Rechenzentrum, oder „die Cloud", übernimmt je nach Produktart nur bestimmte Aufgaben und Pflichten. Unter dem Schlagwort „Shared Responsibility Model" (= Modell geteilter Verantwortung), wird man schnell fündig, wer wofür zuständig ist.

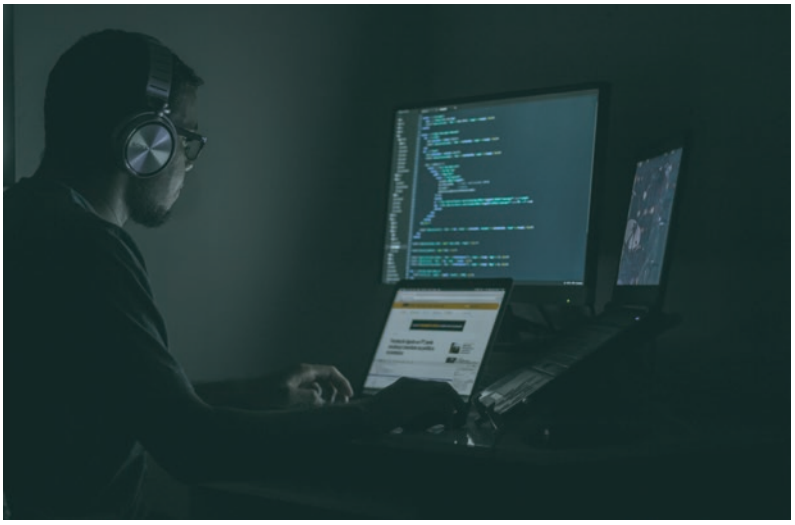
Lesen Sie daher das Groß- und Kleingedruckte, fragen Sie nach und beurteilen Sie kritisch, welche Vor- und Nachteile die Cloud in Ihrem Fall mit sich bringt (z.B. Kosteneinsparungen, Flexibilität, Datenschutzbedenken, Abhängigkeit, ...).

## NOCH EIN WORT ZU PASSWÖRTERN ...

**Haben Sie eine Passwortrichtlinie im Unternehmen?** Orientiert sich diese an der alten oder der neuen NIST-Richtlinie? Wie wird die korrekte Umsetzung überprüft?

Niemand mag Passwörter, das wissen wir. Da ist leider im Juni 2004 viel schiefgegangen. Die NIST-Richtlinie 800-63 „Electronic Authentication Guideline", die den Standard für US-Behörden, US-Hersteller sowie einen Großteil der Welt darstellte, hatte empfohlen, dass Passwörter möglichst komplex sein und oft gewechselt werden sollten. Zum Leidwesen aller Beteiligten. Die Folge waren einfache Zeichenersetzungen (z.B. Null statt 0), durchnummerierte Passwörter, angehängte Rufzeichen und nur wenig zusätzliche Sicherheit. In den darauffolgenden 13 Jahren hat man viel dazugelernt. 2017 wurde die NIST-Richtlinie modernisiert und William Burr, der ursprüngliche Autor, entschuldigte sich sogar öffentlich in einem Zeitungsinterview: „Much of what I did, I now regret."

Seitdem gilt: Länge vor Komplexität, Passwortwechsel nur im Verdachtsfall und weiterhin keine Wörter aus dem Wörterbuch, keine gängigen oder bereits kompromittierten Passwörter.



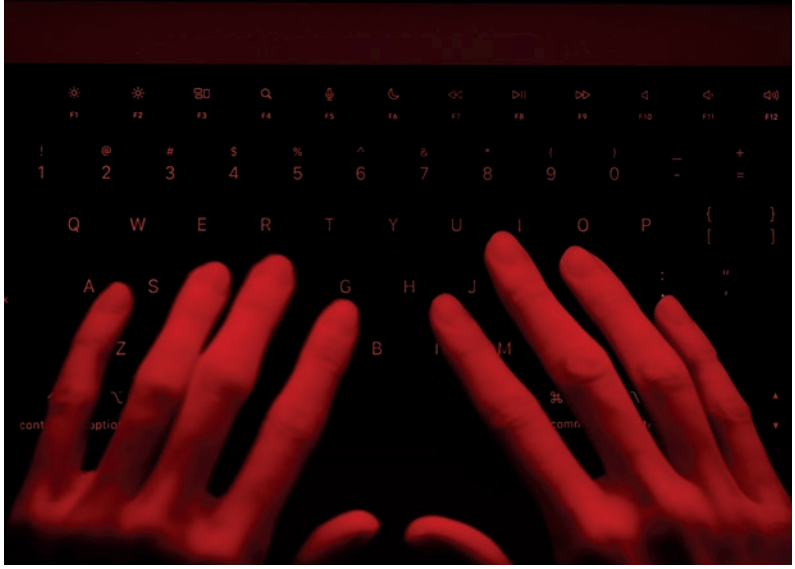
## MEHRFAKTORAUTHENTIFIZIERUNG

**Verwenden Sie Mehrfaktorauthentifizierung** für wichtige und/oder extern erreichbare Zugänge?

Eine weitere Möglichkeit, die zum Glück mehr und mehr Verbreitung findet, ist die Mehrfaktorauthentifizierung. Sie kennen sie vermutlich vom Telebanking, wo man zusätzlich zum Login einen TAN via App oder SMS erhält, um Überweisungen freizugeben. Passwort und TAN stellen zwei separate Faktoren dar – denn die Mehrfaktorauthentifizierung nutzt, wie der Name andeutet, mehrere (unterschiedliche!) Faktoren, um sich anzumelden oder eine Aktion durchzuführen. Dies sichert wichtige Zugänge zusätzlich ab und erschwert, dass diese kompromittiert werden, selbst wenn das obligatorische Passwort gestohlen wurde.

In der IT-Sicherheit unterscheidet man drei Arten von Faktoren: Wissen, Besitz und Biometrie. Jede Faktorart hat gewisse Vor- und Nachteile. So kann Wissen (z.B. Passwort) leicht geteilt, aber auch leicht gestohlen werden. Besitz (z.B. Handy, Smartcard) kann nicht leicht kopiert werden, aber dafür verloren gehen, was man aber wiederum schnell bemerkt. Biometrie (z.B. Fingerabdruck, Gesicht) geht nicht leicht verloren, dafür kann man sie nicht so einfach ändern.

*Foto: Jefferson Santos*



## WER HILFT?

**Kennen Sie das Angebot des cert.at?** Erhalten Sie relevante Newsletter und Informationen? Haben Sie einen erfahrenen IT-Sicherheits-Dienstleister, der Ihnen im Krisenfall zur Verfügung steht?

Mit diesen Voraussetzungen sind Sie bereits ganz gut gewappnet, doch was, wenn doch etwas passiert? Das Wichtigste ist, einen kühlen Kopf zu bewahren. Mit sich überschlagenden Emotionen und Kurzschlusshandlungen vergrößert man den Schaden oftmals. Deshalb: Einmal tief Luft holen, einen Schritt zurück machen und daran denken, dass Sie nicht alleine sind. In fast allen Fällen lohnt sich eine sofortige Kontaktaufnahme mit dem cert.at (Computer Emergency Response Team Österreich). Das CERT bietet nicht nur hochrelevante Newsletter und tagesaktuelle Warnungen vor kritischen Schwachstellen, sondern ist mit seiner Hotline (+43 1 505 6416 78) einfach und unbürokratisch erreichbar.

Die Mitarbeiter*innen des CERTs genießen in der IT-Sicherheitsbranche ein hohes Ansehen, unterstützen tagtäglich unter Beschuss geratene Behörden und Unternehmen mit ihrer ausgereiften Expertise und sind bestens vernetzt – quasi die Dorfältesten des Internets in Österreich.

Eine weitere Anlaufstelle ist die Cyber-Security-Hotline (+43 800 888 133) der WKO. Diese steht rund um die Uhr zur Verfügung, bietet Erstinformationen und -maßnahmen und stellt Kontakt mit einem fähigen IT-Sicherheitsdienstleister her.

Auch eine Anzeige bei der Polizei ist eine sinnvolle Maßnahme. Vermutlich reicht der aktuelle Personalstand nicht für eine rasche, flächendeckende und technisch tiefgehende Soforthilfe, doch sollte man den langen Arm des Gesetzes, insbesondere bei vielleicht österreichischen oder europäischen Täter*innen nicht unterschätzen. Eines ist aber sicher: Ohne Anzeige kommt bestimmt nichts raus.

## NOTFALLPLÄNE UND KRISENSTAB

**Haben Sie Notfallpläne für den Ausfall kritischer Systeme** oder ganzer Standorte (Hochwasser, Feuer, …)? Sind die Zuständigkeiten und Abläufe geklärt? Wissen Sie, wer in Ihrem Krisenstab welche Rolle und Funktion übernehmen wird? Sind all diese Dokumente ausgedruckt verfügbar? Werden sie regelmäßig geübt und aktualisiert oder verstaubt alles nur in einem Schrank?

Seien wir uns ehrlich: Selbst wenn Sie alles richtig gemacht haben, kann trotzdem etwas passieren. Fehler passieren und selbst das ausgeklügeltste System kann überwunden werden. Es macht daher Sinn, sich trotz aller Vorkehrungen auf den Tag der Tage vorzubereiten.

Im Idealfall gibt es für kritische Systeme und Unternehmensstandorte einen Notfallplan. Was wird von wem und wann gemacht, wenn diese ausfallen? Achten Sie dabei auch auf die Priorisierung und Kapazitätenplanung, denn es können mehrere Probleme gleichzeitig auftreten.

Es empfiehlt sich, einen kleinen oder größeren Krisenstab einzurichten. Dieser bündelt im Krisenfall alle Informationen und Verantwortlichen und kann somit effizienter Entscheidungen treffen. Doch achten Sie darauf, dass der Stab schlank und effizient bleibt. Wenn Sie zu viele Leute einbinden, wird Ihr Entscheidungsprozess langsamer. Und wenn Sie Schlüsselpersonal wie IT-Administrator*innen mit Besprechungen binden, wird sich die Problembehebung deutlich verzögern.

In jedem Unternehmen gibt es gewisse Friktionen. Im Krisenfall werden diese erfahrungsgemäß nicht geringer, sondern mehr. Bemühen Sie sich daher um eine gute Zusammenarbeit aller Beteiligten auch im Alltag und üben Sie die Umsetzung der Notfallpläne und die Arbeit im Krisenstab regelmäßig. Denn nicht alles, was auf dem Papier gut klingt, überlebt auch den Kontakt mit der Realität.

## ZUM ABSCHLUSS

Wir hoffen, Ihnen in diesem Artikel einige wertvolle Ideen und Denkanstöße gegeben zu haben. Jedes der angesprochenen Themen ist jedoch ein eigenes Fachgebiet mit eigenen Expert*innen und unzähligen Details. Wir wollen Ihnen daher zum Schluss noch eines mitgeben: Seien Sie mutig und nehmen Sie das Thema in Angriff. Es gibt viele gute Expert*innen, die Ihnen gerne helfen. Selbst ein weniger als perfekt umgesetzter Plan ist besser, als den Kopf weiter in den Sand zu stecken. In diesem Sinne: Alles Gute und viel Erfolg im digitalen Westen! ■

Foto: Wesley Tingey