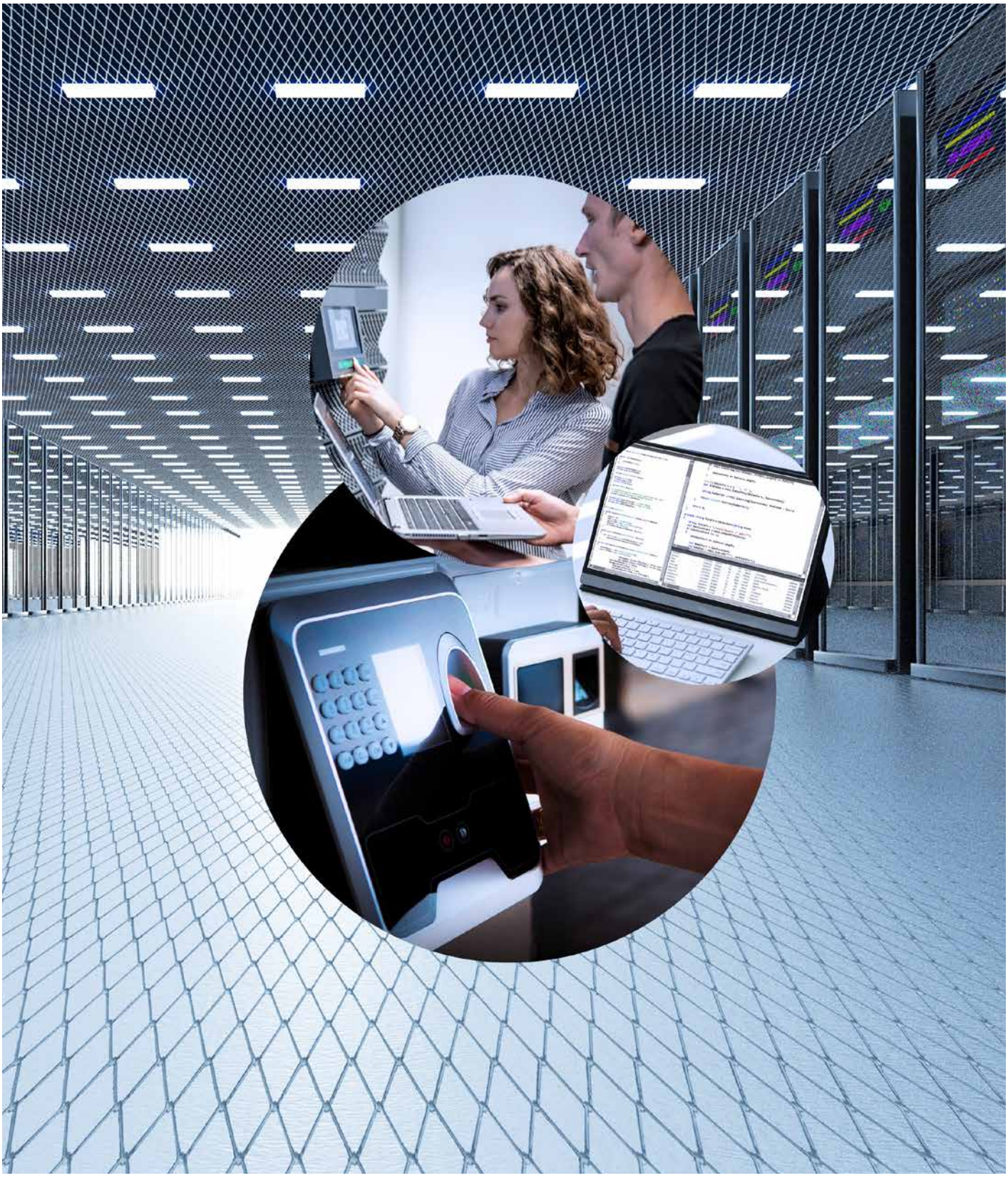
valantic

WHITEPAPER | IT-SECURITY



Katastrophenfall: Cyber-Angriff

Das ist zu tun, wenn der K-Fall eintritt

Inhalt

Vorwort

Die INTARGIA Managementberatung, eine hundertprozentige Tochter der valantic, berät Kunden immer dort, wo sowohl IT- als auch Business-Know-how gefragt sind. Von **A wie Anwendungsfall** bis **Z wie Zugriffskontrollen**. Außerdem spielt das Thema **Datenschutz** eine sehr wichtige Rolle. Wir sind aktuell von über hundert Unternehmen als externer Datenschutzbeauftragter bestellt.

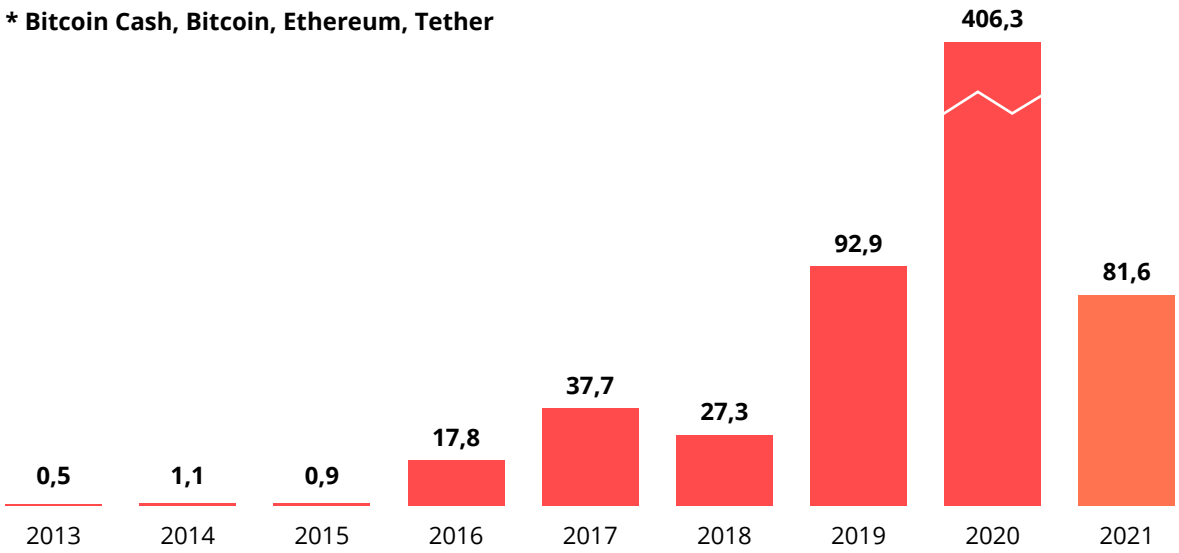
In diesem Whitepaper möchten wir Ihnen am Beispiel eines real erfolgten, aber anonymisierten **Cyber-Angriffs** die Gelegenheit bieten, aus den Erfahrungen anderer zu lernen. Dabei ging es um einen typischen deutschen Hidden Champion, welcher **Opfer eines Ransomware-Angriffs** wurde. Ransomware – abgeleitet vom englischen Wort „ransom" für „Lösegeld", auch als Erpressungstrojaner, Erpressungssoftware oder Verschlüsselungstrojaner bezeichnet – hatte in diesem Fall die IT-Systeme verschlüsselt und damit unbrauchbar gemacht.

Schnell war klar, es bedurfte eines erfahrenen Partners, um den Angriff zu analysieren und die Systeme wieder ans Laufen zu bringen. Leider kein ganz seltenes Ereignis im Jahr 2020/21, wie die Grafik von Statista zeigt. So sind allein im letzten Jahr mehr als 400 Mio. US-Dollar an Lösegeld in Form von Kryptowährungen gezahlt worden. In diesem Jahr beläuft sich die Summe bereits fast auf den Gesamtbetrag des Jahres 2019. Die Bedrohung scheint also stetig zuzunehmen.

Das lukrative Geschäft mit dem Online-Lösegeld

Volumen der an Ransomware-Adressen gezahlten Kryptowährung (in Mio. US-Dollar)*

*** Bitcoin Cash, Bitcoin, Ethereum, Tether**



Quelle: chainalysis.com; Stand: 10. Mai 2021

Denn inzwischen sind auch sehr namhafte und bekannte Unternehmen als auch viele Behörden von Cyber-Kriminalität und IT-Angriffen betroffen. Ein Blick in die täglichen Schlagzeilen der Tageszeitungen lässt das Ausmaß erahnen: „Mehr als 100 Behörden erpresst“ las man etwa im Juli 2021 auf der Seite der tagesschau, und der Bayrische Rundfunk titelte im Mai 2021: „Ransomware-Angriffe: Cyberkriminelle sind aufs große Geld aus“. Und die Dunkelziffer dürfte noch viel größer sein, denn keiner der Betroffenen hängt derartige Vorfälle gerne an die große Glocke.

Falls Ihr Unternehmen vorsorgen möchte, um einem wie in diesem Whitepaper beschriebenen Szenario zu entgehen, oder Sie vielleicht sogar gerade von einem Cyberangriff betroffen sind, so helfen wir Ihnen umgehend mit unserer Expertise und Erfahrung weiter. Sprechen Sie uns gerne an.

Bleiben Sie wachsam!

Ihr Thomas Lang

Thomas Lang
Geschäftsführender Partner bei der
INTARGIA Managementberatung GmbH –
a valantic company
thomas.lang@intargia.com

Nach über 20 Jahren als Berater und Unternehmer ist für Thomas Lang das schnelle Einarbeiten auch in kritische Situationen in „Fleisch und Blut“ übergegangen. Er bewahrt in jeder Lage Ruhe, kann Wichtiges von Unwichtigem trennen und gibt Dingen Struktur. Das hilft ihm, um in schwierigen Situationen den Überblick zu bewahren. Zu seinen Beratungsschwerpunkten gehören neben den Themen IT-Security & Compliance unter anderem die Themen IT-Strategie, Projekt-Governance und -Controlling, Krisenmanagement sowie IT-Infrastruktur & Betrieb.

Ein ganz normaler Morgen...

Häufig geht es damit los, dass die IT-Abteilung Unregelmäßigkeiten am frühen Morgen erkennt. Zu diesem Zeitpunkt glaubt noch niemand, dass ihm so etwas wirklich selbst passieren könnte. Bis die bittere Erkenntnis eintritt und es zum ersten „Aha-Erlebnis“ kommt: **Wir sind Opfer eines Cyber-Angriffs geworden**. Schnell werden Netzwerkverbindungen getrennt, Systeme heruntergefahren und die Vorgesetzten beziehungsweise die Unternehmensleitung informiert.

Im weiteren Verlauf der Realitätsbewältigung klingelte dann das Telefon der Berater*innen von INTARGIA. Gewünscht wurden konkrete Handlungsweisen, Kontakte zu Forensik-Fachleuten und aktives Krisenmanagement. Bei Anrufen dieser Art ist eines klar: Es muss sehr schnell gehen. In der Regel wird ein*e Berater*in direkt vor Ort angefordert.

Nach dem ersten Schock

Spurensicherung und Tathergang dokumentieren

Am Ort des Geschehens ist eine gewisse Anspannung greifbar. Auf dem Weg in den Besprechungsraum, der in den nächsten Tagen zum „**Cyber War Room**" umfunktioniert wird, geht es durch offene und festgestellte Türen – Zutrittskontrollsysteme sind meist ausgefallen – und vorbei an verwaisten Arbeitsplätzen. Man bekommt einen ersten Eindruck, dass hier wohl gerade gar nichts mehr geht.

Danach geht es möglichst strukturiert los:

- Namen und Rollen werden notiert
- Was ist passiert – Reihenfolge, zeitlicher Ablauf?
- Wer hat wann was genau gemacht?
- Liegt ein Erpresserschreiben vor?
- Wer wurde wie, wann, von wem und mit welchem Inhalt informiert (Kunden, Geschäftspartner, Behörden)?
- Welche Form von Backups steht zur Verfügung?
- Wann hat das letzte „saubere" Backup, zum Beispiel durch Auslagerung von Bändern, stattgefunden?

Diese und weitere Fragen werden gestellt und konzentriert abgearbeitet. Denn eines ist klar: Jede Minute kostet Geld.

Hintergrundinfo:

Im Juli 2021 wurden die Daten Hunderter Unternehmen weltweit durch eine Ransomware-Krypto-Attacke unbrauchbar gemacht. Dem Vernehmen nach steckt die Cybergruppe REvil hinter dem groß angelegten Angriff. REvil bietet im Darknet die Dienstleistung Ransomware-as-a-Service (RaaS) an, fast so bequem wie Office 365 aus der Cloud, Salesforce Marketing oder der Apple Store. Die technologischen Hürden für Cyberkriminelle, einen Ransomware-Angriff durchzuführen, sind drastisch gesunken.

Quellen: (1) REvil: Einblicke in Ransomware-as-a-Service, (2) Hackergruppe REvil erpresst bis zu 1500 Unternehmen

Welche Maßnahmen sind wichtig?

In den genannten Fällen wurden annähernd alle wesentlichen Systeme verschlüsselt. Folglich stand der Geschäftsbetrieb zu diesem Zeitpunkt komplett still. Hunderte bis Tausende von Mitarbeitenden wurden nach Hause geschickt und Kundenaufträge konnten nicht bearbeitet werden. Nicht nur die Uhr tickt, vor allem der „Geldzähler" läuft. Aktuell kostet jede Minute richtig viel Geld, und Geld ist an dieser Stelle ein gutes Stichwort. Die Erpressenden fordern Lösegeld, erst dann werden die Systeme entschlüsselt und sind wieder nutzbar.

Weitere Fragen drängen sich auf:

- Hat sich Ihr Unternehmen mit der Frage, wie in einem Erpressungsfall verfahren wird, schon beschäftigt?
- Gibt es Regelungen für den Fall, dass Angehörige der Eigentümerfamilie betroffen sind oder sogar mit der Verunreinigung von Produkten gedroht wird?

- Ist den Geschäftsführungs- und Vorstandsmitgliedern bewusst, dass sie nach der Zahlung von Lösegeld im Darknet als „zahlendes Opfer" gelistet werden?
- Hat Ihr Unternehmen ein Bitcoin-Konto?
- Wollen Sie die Behörden einschalten (Kripo, das LKA oder gar den Verfassungsschutz)?

Es dauert einige Zeit, bis den verantwortlichen Personen das Ausmaß und die potenzielle Bedrohung klar wird. Zudem müssen die Berater*innen von INTARGIA auf die 72-Stunden-Frist hinweisen, innerhalb derer nach Bekanntwerden eines Data Breaches eine Meldung an die Datenschutzbehörde erfolgen muss.

Hintergrundinfo:

Anfang Juni 2021 wurde der weltgrößte Fleischkonzern JBS aus Brasilien Opfer einer Ransomware-Attacke. Fünf der größten Fleischfabriken in den USA wurden zeitweise durch Verschlüsselungstrojaner stillgelegt. Eigentlich gilt bei Ransomware-Angriffen die eiserne Regel, den Forderungen der Erpresser*innen nicht nachzugeben. Der Konzern entschloss sich jedoch zu einer Lösegeldzahlung von 11 Millionen Dollar, um seine Anlagen möglichst schnell wieder in Betrieb nehmen zu können. Die Zahlung erfolgte in der Kryptowährung Bitcoin.

Quelle: Meat giant JBS pays $11m in ransom to resolve cyberattack

Zahlen oder nicht zahlen?

Bei einem Ransomware-Angriff mit Lösegeldforderung stellt sich immer die entscheidende Frage: Zahlen oder nicht zahlen? Kann die eigene IT auch ohne Lösegeldzahlung vollständig wieder hochgefahren werden? Den betroffenen Unternehmen stehen zwei Optionen zur Auswahl:

Das No-Pay-Szenario – Vorteile und Nachteile

Das No-Pay-Szenario geht davon aus, dass das Unternehmen den Re-Start seiner IT-Systeme selbst übernimmt, indem die infizierten Systeme gesäubert und vorhandene Backups eingespielt werden. Eine sehr gründliche Vorgehensweise ist dabei besonders wichtig. Auch wenn Sie alle Systeme aus dem Backup wiederherstellen können, bestünde die Gefahr, dass die Angreifenden nach wie vor einen Schlüssel im System versteckt haben – Stichwort: **Golden Ticket**. Dieser Gefahr will sich kein Unternehmen aussetzen, weshalb die Neuinstallation aller Systeme in Verbindung mit modernen Abwehr- und Containment-Systemen in der Regel unvermeidbar ist.

Das Pay-Szenario – Vorteile und Nachteile

Das Pay-Szenario sieht vor, dass die Erpresser*innen bezahlt werden, wichtige Systeme völlig abgeschottet von der neuen Umgebung wieder in Betrieb genommen und Daten „handverlesen" in das neue System übernommen werden. Denn auch hier ist klar, dass **ein System, in dem eine fremde Person einmal administrative Rechte hatte, nie wieder Ihr volles Vertrauen genießen wird**.

Nun fragen Sie sich vielleicht, warum überhaupt jemand auf die Idee kommen könnte, an Erpresser*innen zu zahlen? In einem der vorliegenden Fälle sah die Situation wie folgt aus:

- Backups erfolgten täglich auf Disk – aber alle Disks waren verschlüsselt

- Wöchentliche Backups erfolgten auf Bändern

- Monatlich wurden Bänder aus der Tape Library entnommen und eingelagert

Nach eingehender Analyse stellte sich heraus, dass eine Datenlücke von drei Wochen nicht überbrückt werden konnte. Die Angreifenden waren mehrere Wochen im Netz unterwegs und hatten sehr viel Zeit darauf verwendet, jedes einzelne in der Tape Library vorhandene Band einzulegen und zu löschen. Das Unternehmen hatte just in den vergangenen Wochen massivste Produktentwicklung und Vorplanung betrieben. Selbst ein auf **Datenrettung** spezialisiertes Unternehmen konnte die gelöschten Bänder nicht wiederherstellen, sodass den Vorstandsmitgliedern letztlich nur eine Entscheidung blieb: wir bezahlen.

Und das sollte man sich im Übrigen nicht zu einfach vorstellen. Zwischen der ersten Kontaktaufnahme mit den Erpresser*innen und der Bereitstellung des Schlüssels für Ihre Daten können durchaus einmal 48 bis 72 Stunden liegen.

Zwei weitere Dinge sind an dieser Stelle zu bedenken:

1. Die Entschlüsselung der Daten wird – je nach Datenmenge – mehrere Tage in Anspruch nehmen.

2. Wie schnell wären Sie in der Lage, für eine sechs- bis siebenstellige Summe Bitcoin zu besorgen? Es gibt zwar Börsen, an denen man Kryptowährungen erwerben kann. Aber dort gelten die Gesetze des Marktes, nach denen die Nachfrage den Preis bestimmt. Es ist also ratsam, in vielen kleineren Margen einzukaufen, um nicht den eigenen Preis hochzutreiben. Auch das kostet Zeit.

Hintergrundinfo:

Regelmäßig durchgeführte Backups können vor Datenverlusten und unbrauchbaren Daten schützen. In der Regel wird lediglich anfangs ein zeitaufwendiges Voll-Backup nötig. Danach reicht es, das sogenannte Delta, also die seit dem letzten Backup geänderten oder neu hinzugekommenen Daten, zu sichern. Wichtig ist, die Backups regelmäßig durchzuführen und ohne Netzanbindung an die produktiven IT-Systeme aufzubewahren, damit im Falle einer Cyber-Attacke die Backups nicht ebenfalls infiziert werden.

Vorkehrungen für den Katastrophenfall

Eine spannende Geschichte, oder? Bleibt die Frage, wie man solche Situationen verhindert und sich auf den nicht auszuschließenden Katastrophenfall vorbereiten kann.

Dabei sind einige Vorkehrungen zu treffen und einige Fragen vorab zu klären:

- Wollen Sie den Forderungen der Erpresser*innen nachgeben: zahlen oder nicht zahlen?
- Business Continuity Management (BCM): Gibt es ein Sicherheitskonzept und Notfallpläne für die Aufrechterhaltung der Produktion und der Betreuung von Kundenanfragen?
- Sind das Krisenmanagement und die Kommunikation inklusive der Verantwortlichkeiten im K-Fall strukturiert?
- Ist im K-Fall eine schnelle Abschottung und Wiederherstellung der betroffenen Systeme gewährleistet?
- Ist Ihr Unternehmen für die Spurensicherung und Dokumentation des Tatzeithergangs gut gerüstet?

Hintergrundinfo:

Cloud-Provider und Rechenzentrumsbetreiber bieten ihren Kunden in der Regel - abgestimmt auf die individuellen Anforderungen - abgestufte Sicherheitskonzepte an. Sehr sicher, aber auch kostenintensiv, ist die komplette, geo-redundante Spiegelung der Daten auf die Speichermedien eines zweiten Rechenzentrums. Vor sogenannten Schläfern, also Krypto-Trojanern, die erst ab einem bestimmten Datum in der Zukunft tätig werden, schützt aber auch die geo-redundante Spiegelung kaum. Denn der „Schläfer" wurde bereits auf das zweite Backup-Rechenzentrum gespiegelt und macht auch dort die Daten unbrauchbar. Das kann Ihnen übrigens auch mit Backup Tapes passieren. Beim nächsten „Restore" wacht der „Schläfer" auf und befällt die Daten auf den Backups.

Update zum obigen K-Fall:

Cyberkriminelle erhöhen den Druck auf Unternehmen

In den letzten Monaten haben Cyberkriminelle ihr Erpresserpotenzial massiv ausgeweitet. Sie verschlüsseln nicht nur die Daten des angegriffenen Unternehmens und machen sie dadurch für die weitere Benutzung unbrauchbar. Zusätzlich werden sensible Daten wie Mitarbeiter*innen-Dateien, Konstruktionspläne oder Marktstrategien, die nicht in die Hände der Konkurrenz fallen sollten, entwendet. Dadurch erhöht sich der Druck auf die betroffenen Unternehmen enorm, denn die Angreifenden halten gleich mehrere Trümpfe in der Hand.

Mögliche Schäden betreffen nicht nur die kompromittierten Unternehmen selbst. Haben sich Cyberkriminelle etwa der Ausweiskopien von Mitarbeiter*innen auf den HR-Servern bemächtigt, dann könnten diese sensiblen Informationen zum Beispiel von Schleuserbanden dazu benutzt werden, gefälschte Papiere für Flüchtlinge zu erstellen, um ihnen die illegale Einreise zu ermöglichen. Auch Geheimrezepte für beliebte Fitness Drinks, Blaupausen für Innovationen oder andere stark marktrelevante Daten sollten besser nicht in unbefugte Hände fallen.

Unternehmen sind diesen Risiken jedoch nicht schutzlos ausgeliefert. Mit künstlicher Intelligenz ausgestattete Virenscanner der neuesten Generation, die Endgeräte und IT-Systeme 24x7 überwachen und bei Anomalien Alarm schlagen, bieten bereits einen hohen Schutz. Unter anderem heuristische Wahrscheinlichkeitsberechnungen, typische Auslastungsszenarien und Abweichungen vom typischen User-Verhalten spielen dabei eine Rolle. Meistens gelingt es, die eingedrungene Malware oder Ransomware zu isolieren, ein Übergreifen auf weitere IT-Subsysteme zu verhindern und den Schaden zu minimieren. Unternehmen sollten ihre Verteidigungsstrategie so weit wie möglich optimieren. valantic empfiehlt, technische Methoden der Angriffsbekämpfung gezielt mit organisatorischen Maßnahmen zu kombinieren. Schlägt zum Beispiel ein KI-Scanner Alarm, sollte ein*e menschliche*r Security-Expert*in innerhalb kürzester Zeit weitergehende Abwehrmaßnahmen einleiten sowie das Management und die Mitarbeiter*innen informieren. Dadurch lassen sich größere Schäden in der Regel wirksam vermeiden.

Fazit

Das Thema Cyberkriminalität ist in diesen Zeiten so real wie noch nie, die Fallzahlen steigen stetig an und die Lösegeldsummen, wie beispielsweise bei Ransomware-Angriffen, werden immer höher. Daher ist es ratsam, sich schon vor einem etwaigen Angriff Gedanken über ein umfassendes **Sicherheits- und Krisenmanagement- sowie Business-Continuity-Konzept** zu machen und Vorkehrungen zu treffen, wie im K-Fall reagiert werden sollte.

Wenn Sie mehr erfahren wollen, wie Sie auch Ihr Unternehmen effizient schützen können, dann stehen wir Ihnen für ein unverbindliches Gespräch sehr gerne zur Verfügung.

Jetzt Kontakt aufnehmen

INTARGIA Managementberatung GmbH – a valantic company

+49 6103 50 86 0

info@intargia.com
www.intargia.com

Dreieich Plaza 2A
63303 Dreieich
Deutschland

www.valantic.com
November 2021