IT-SICHERHEIT: HEUTE UNVERZICHTBAR FÜR JEDES UNTERNEHMEN

Cyberangriffe sind eine wachsende Bedrohung – So schützen Sie sich

Texte: Susanne Rendenbach,
Fotos: Christopher Arnoldi (S. 8, 9, 10, 11), IHK Trier (S. 9),
Sandra - stock.adobe.com - generiert mit KI (S. 12), Vidio – stock.adobe.com (S. 13)

JEDES SIEBTE UNTERNEHMEN WURDE 2024 OPFER EINES CYBERANGRIFFS. BEI ALLEN BETROFFENEN HAT DIES ZU EINEM UMDENKEN BEIM THEMA IT-SICHERHEIT GEFÜHRT, BERICHTEN EXPERTEN. GENERELL WERDE DAS THEMA INDES STRÄFLICH VERNACHLÄSSIGT.

Horst Schäfer, Geschäftsführer von save IT first, kennt die Gefahren durch Cyberkriminalität und nennt mögliche Lösungen (siehe Interview S. 10/11).

Markus Golembiewski von save IT first im Serverraum des Unternehmens.

Es ist der Gau für jedes Unternehmen und trifft diese so gut wie immer an einer ihrer empfindlichsten Stellen: Ein Hackerangriff – auch Cyberangriff genannt – kann nicht nur zu großer Verunsicherung, Chaos und einer Vertrauenskrise auf unterschiedlichen Ebenen führen. Im schlimmsten Fall – und der tritt häufiger ein, als es sich mancher vorstellen mag – legt eine Netzattacke entscheidende Bereiche des Unternehmens für Tage und Wochen lahm und verursacht in der Folge mitunter einen immensen wirtschaftlichen Schaden.
Der Begriff Hacking tauchte erstmals in den 70er-Jahren auf und „bezeichnet den Missbrauch von Geräten wie Computern, Smartphones, Tablets und Netzwerken, um Systeme zu beschädigen oder zu korrumpieren, Informationen über Benutzer zu sammeln, Daten und Dokumente zu stehlen oder datenbezogene Aktivitäten zu stören“. So lautet die Beschreibung des weltweit agierenden US-amerikanischen Cybersecurity-Anbieters Fortinet.

Sensibilität für Thematik zu wenig ausgeprägt

Dabei betrifft das Thema Netzkriminalität beziehungsweise Netzsicherheit längst jedes Unternehmen – völlig unabhängig von der Branche, Unternehmensgröße oder Region. Dass dem so ist, darin sind sich die Experten ebenso einig wie in der Einschätzung, dass das Bewusstsein und die Sensibilität hinsichtlich der Thematik bis dato sehr schwach ausgeprägt sind (siehe auch die Beiträge auf den Seiten 10-13).
„Viele denken: ‚Uns betrifft das nicht‘, beschreibt Christian Kien, Referent Innovation, Digitalisierung, Energie der IHK Trier, die vorherrschende Haltung. „Tatsächlich betrifft es vom Selbstständigen ohne Mitarbeiter bis zu Großunternehmen mit einer großen Belegschaft jedes Unternehmen. Jeder, der Daten auf einem Gerät hat, muss das Thema auf dem Schirm haben.“
Statt sich auch mit dem Thema IT-Sicherheit auseinanderzusetzen, dafür intern Personal abzustellen beziehungsweise externe Expertise hinzuzuziehen und ein IT-Budget einzuplanen, setzten viele die Priorität beim Tagesgeschäft. „Wie wichtig das Thema ist und wie existenziell bedrohlich es ohne entsprechende Vorkehrungen werden kann, wird den meisten erst klar, wenn etwas passiert. Solange nichts passiert, hat man scheinbar nichts damit zu tun. Wenn der Hacking-Fall eintritt, brechen große Betroffenheit und Panik aus.“

Bewusstsein für Umgang mit Daten schaffen

Nach Kiens Erfahrung versuchen die meisten Unternehmen, ein Hacking unter Verschluss zu halten. Der Hauptgrund für die Geheimhalte-Taktik liegt auf der Hand: Es ist die Angst davor, dass die Reputation des Unternehmens Schaden nimmt. Die Angst vor einem Vertrauensverlust bei Kunden, Lieferanten, kooperierenden Partnern.
Als Haupteinfallstor für einen erfolgreichen Angriff macht Kien – wie die übrigen für dieses Titelthema Befragten – die Mitarbeitenden aus. „Vom Praktikanten bis zur Geschäftsführung muss jeder Mitarbeitende im Unternehmen das Bewusstsein und Verständnis dafür entwickeln, wie Datenflüsse und digitale Prozesse funktionieren, zusammenhängen, welche Rolle sie im und für das Unternehmen spielen und was sie bewirken. Deshalb sollten Mitarbeiter auch regelmäßig in diesem Bereich geschult werden. Das beinhaltet auch, ihnen den Sinn und die Relevanz dieser Schulungen zu vermitteln.“

Christian Kien ist Referent Innovation, Digitalisierung, Energie bei der IHK Trier.

Früher im Tresor, heute im Computer

Auf die Frage, was er Entscheidern/Unternehmern gerne nahebringen würde, antwortet Kien: „Dass sie die Wichtigkeit des Themas höher hängen! Es kostet Zeit, Aufwand und Geld, IT-Sicherheit im Unternehmen zu implementieren, um sich bestmöglich vor Angriffen zu schützen. Aber wie teuer wäre vergleichsweise ein wochenlanger Produktionsausfall, weil die kompletten Daten verschlüsselt wurden und nicht mehr zugänglich sind? Früher war es der Tresor, in dem das Unternehmen besonders wertvolle Dinge aufbewahrte. Heute ist es der PC mit seinen Daten. Und die Methoden, mit denen Kriminelle versuchen, an sie heranzukommen, werden immer trickreicher.“

Jedes siebte Unternehmen wurde 2024 gehackt

Trierer IT-Dienstleister „save IT first“ im Interview

Horst Schäfer ist gemeinsam mit Marco Becker Geschäftsführer des Trierer IT-Dienstleisters „save IT first“. 2011 gegründet, lag der Schwerpunkt von Beginn an auf IT-Security. Inzwischen beschäftigt die Firma 27 Mitarbeiter und betreut Kunden deutschlandweit. Blickpunkt Wirtschaft hat mit Horst Schäfer darüber gesprochen, welchen Stellenwert IT-Sicherheit in Unternehmen hat, welche Risiken es durch Hackerangriffe gibt und wie sich Unternehmen bestmöglich davor schützen können.

In jüngster Zeit ist immer häufiger von Cyberangriffen auf Unternehmen, Einrichtungen und öffentliche, mitunter sensible Infrastruktur zu hören. Was die Unternehmen betrifft: Gibt es Branchen, die besonders anfällig für Angriffe sind?

Nein. Das Problem ist branchenunabhängig. 2024 war in Deutschland jedes siebte Unternehmen von einem Hackerangriff betroffen. Der wirtschaftliche Gesamtschaden betrug 180 Milliarden Euro. Auch die Größe eines Unternehmens ist nur bedingt relevant. Allerdings ist unsere Erfahrung: Je kleiner das Unternehmen, desto höher die Wahrscheinlichkeit, dass die IT nicht ausreichend geschützt ist. Es gibt aber auch Betriebe mit 100 Mitarbeitern, in denen eine einzige Person für die IT zuständig ist. Das kann nicht funktionieren.

Klingt, als fehle es auf Unternehmensseite an Bewusstsein für die Problematik.

In der Tat ist es ein Mindset-Problem. Wenn Sie als Unternehmer einen Neubau planen, haben Sie hierzulande hohe Brandschutz-Auflagen zu erfüllen. Was die IT betrifft, gibt es das nicht. Unternehmen sichern sich gegen Feuer-, Wasser-, Sturm- und Hagelschäden ab. Die Bereitschaft, in IT-Sicherheit zu investieren, ist hingegen häufig sehr gering. Da wird eher ein teurer Firmenwagen oder ein teures I-Pad angeschafft. „Bei uns ist doch nichts zu holen”, lautet oft das Argument.

Was setzen Sie dem entgegen?

Man muss verstehen, dass es mittlerweile eine globale Industrie gibt, die mit Hacking ihr Geld verdient. In Nordkorea beispielsweise füllt das die Staatskasse. 2024 hat sich der Staat allein mit dem Diebstahl von Krypto-Währung um 1,3 Milliarden Dollar bereichert. Ziel der diversen Angriffe ist grundsätzlich jeder, der mit seiner IT als verwundbar zu identifizieren ist.

Dabei steckt ja nicht immer ein korrupter Staat hinter den Angriffen.

Es ist immer die Frage, was die Intention von Cybercrime ist. Wollen die Angreifer Geld verdienen? Geht es um das Zerstören der Reputation eines Unternehmens? Es gibt die gezielten Angriffe ebenso wie die wahllosen, bei denen Einzeltäter ebenso wie organisierte Banden ausprobieren wollen, ob das Hacking funktioniert. Und das machen sie so lange, bis sie irgendwo eine Schwachstelle ausgemacht und geknackt haben. Dabei hilft ihnen inzwischen die Künstliche Intelligenz (KI), mit der sich ohne spezielles Know-how hochintelligente Schädlings-Software bauen lässt.

Gibt es – was die unterschiedlichen Formen der Angriffe betrifft – eine Methode, die besonders häufig angewendet wird?

60 Prozent der geschädigten Unternehmen sind von Ransomware-Angriffen betroffen. Dabei werden die Geräte mit einer schädlichen Software so manipuliert, dass der Zugang gesperrt ist und alle gespeicherten Daten verschlüsselt werden. In der Regel geht der Angriff mit einer Lösegeldforderung und der vermeintlichen Zusage einher, bei Zahlung

Die Geschäftsführer Marco Becker und Horst Schäfer (von links) vor ihrem Firmensitz von save IT first auf dem Trierer Petrisberg.

eine Entschlüsselungssoftware zu erhalten – was sich häufig als leere Versprechung entpuppt.

Das heißt, Sie raten davon ab, auf Lösegeldforderungen einzugehen?
Ja! Das zeigt den Hackern nur, dass sie auf jemanden getroffen sind, der bereit ist zu zahlen. Das Unternehmen ist am Ende eine Menge Geld los und kommt womöglich trotzdem nicht an seine Daten heran.

Welches ist die größte Schwachstelle innerhalb eines Unternehmens?
Der Mensch. Vieles beginnt mit dem Mitarbeiter, der aufgrund unzureichender Kenntnisse und mangelnder Affinität zum Thema unbedacht Fehler macht. Dabei ist diese Schwachstelle am einfachsten zu beheben und hat den größten Effekt. Vorausgesetzt, die Geschäftsführung hat verstanden, wie wichtig das Thema ist. Sie muss die Belegschaft mit ins Boot nehmen, sie für das Thema sensibilisieren und mit wiederkehrenden Schulungen fit machen und auf dem neuesten Stand halten.

An welcher Stelle passieren Fehler?
Das Haupteinfallstor für Hacker sind zu 90 Prozent E-Mails. Von daher sind bestimmte Sicherheitslösungen für Hard- und Software dringend geboten, und man sollte den aufmerksamen Umgang beim E-Mail-Verkehr vermitteln. Ebenso wichtig ist ein stringentes Berechtigungsmanagement, gerade auch im Hinblick auf das Homeoffice. Das bedeutet, dass – entsprechend dem jeweiligen Arbeitsplatz und der Aufgabe – für jeden einzelnen Mitarbeiter der digitale Bewegungsspielraum sehr genau definiert und durch spezielle Software begrenzt wird. Wenn jeder Zugang zu allen Datenbanken, Internetseiten, Mailadressen etc. hat, erhöht das das Risiko, dass unwissentlich Schadsoftware eingeschleust wird.

Wo liegen weitere Risiken?
Häufig ist die Hardware völlig veraltet. In großen Unternehmen werden mit gutem Grund alle drei Jahre die PC ausgewechselt. Darüber hinaus müssen die Systeme aktuell gehalten werden. Elementar ist Datensicherung, die periodisch getestet und angewendet wird. Ganz wichtig ist zudem eine Notfallplanung, die explizit beschreibt, wer was bei einem Angriff zu tun hat und auch die externen Ansprechpartner klar definiert.

Wie sollte das Unternehmen bei einem Angriff akut reagieren?
Zunächst einmal: unbedingt einen kühlen Kopf bewahren und nichts Unbedachtes aus dem Affekt heraus tun! Dann gilt es, das infizierte System zu identifizieren und zu isolieren. *(Weitere Infos auf Seite 13)*

Was sind Schritte, um IT-Sicherheit bei einem Neukunden zu implementieren?
Zusammengefasst konzentrieren wir uns zunächst auf folgende Kernpunkte: Wie arbeitet das Unternehmen? Welches sind die Kronjuwelen, und welche Prozesse müssen auf jeden Fall funktionieren? Ganz wichtig ist die Verhältnismäßigkeit. Man muss nicht mit Kanonen auf Spatzen schießen. Unser Slogan lautet: „IT-Sicherheit braucht Strategie". Es geht nicht allein um technische, sondern auch um organisatorische Fragen im Unternehmen. Das ist viel Fleißarbeit.

Was ist Ihre Prognose, wie wird sich das Thema Cybercrime entwickeln?
Wir erleben aktuell auf sehr unterschiedlichen Ebenen, wie präsent das Thema ist. KI wird das Problem intensivieren. Es gibt schon heute KI-gestützte Angriffe, die extrem intelligent gemacht und gefährlich sind. Von daher kann ich nur jedem ans Herz legen, sich mit Cybersicherheit zu befassen und zu prüfen, wo sich Schwachstellen beheben und Schlupflöcher schließen lassen. Das Thema wird uns in der Zukunft vermehrt beschäftigen.

Geschäftsführer Marco Becker berät mit save IT first Unternehmen zur IT-Sicherheit.

„Wir sind Partner, keine Bremsklötze“

Frank Birk leitet das Kommissariat Cybercrime bei der Kripo Trier

„Es ist inzwischen keine Frage mehr, ob ein Unternehmen von Cyberkriminellen angegriffen wird, sondern nur noch, wann es angegriffen wird.“ Diese ernüchternde Feststellung trifft Frank Birk, Leiter des Kommissariats Cybercrime bei der Kriminalpolizei (Kripo) Trier, im Gespräch mit Blickpunkt Wirtschaft.

Das Thema Cybercrime sei längst in der Region angekommen. Viele Unternehmen hätten damit bereits leidvolle Erfahrung gemacht. Dabei ist Birk überzeugt: „Wir müssen mit einer erheblichen Dunkelziffer rechnen, da sehr viele Unternehmen einen Angriff aus Angst vor Reputationsverlust bei Kunden, Zulieferern oder Geschäftspartnern nicht zur Anzeige bringen.“

Spionage auf politischer und wirtschaftlicher Ebene

Die Bandbreite der Angriffe scheint so unbegrenzt wie das Internet selbst. „Wir haben mit Staaten zu tun, die uns aushorchen.“ Spionage auf politischer Ebene sei ebenso an der Tagesordnung wie klassische Industrie-Spionage. „Die Chinesen sind Weltmeister im Kopieren.“ Als Beispiel beschreibt Birk den Vorfall bei einem Unternehmen aus der Region, das global erfolgreich mit einem High-Tech-Produkt unterwegs ist. Dort waren vor einiger Zeit die Daten komplett kopiert worden.

„Nord-Korea bedient in punkto Cybercrime alle Bereiche, die man sich überhaupt vorstellen kann. Und das mit hochqualifizierten, im asiatischen und pazifischen Raum top-ausgebildeten Leuten.“ Neben sich stetig stärker verbreitenden Phänomenen wie Datenklau, Datenverschlüsselung, Sabotage und Spionage zeichne sich mit dem sogenannten CEO-Fraud ein immer wiederkehrender Trend ab.

Betrüger sammeln Infos zum Unternehmenschef

Beim CEO-Fraud sammeln die Täter über unterschiedliche Kanäle (Website, Interneteinträge, Anrufe im Unternehmen mit gezielten Nachfragen zum Chef) Infos zu dem von ihnen ausgespähten Unternehmenschef. Über generierte E-Mail-Adressen oder einen kopierten Geschäftspapierbogen nehmen sie Kontakt mit einem Firmenmitarbeiter auf und veranlassen als vermeintlicher Geschäftsführer einen Geld-Transfer ins Ausland.

„Diese Aktionen laufen meistens freitagnachmittags, sodass bei den Banken niemand mehr erreichbar ist, wenn die Täuschung im Unternehmen aufgefallen ist. Die Summen werden sofort gesplittet und häufig in den arabischen und asiatischen Raum in Kryptowährungen transferiert.“

Im Einvernehmen mit Firma digitale Spuren ermitteln

Dass so viele Unternehmen Cyber-Angriffe nicht bei der Kripo anzeigen, liegt für Birk primär am befürchteten Vertrauensverlust. Darüber hinaus erklärt er es mit einer Fehleinschätzung dahingehend, wie die Polizei im Ernstfall auftritt. „In einer solchen Situation herrscht Chaos im Unternehmen. Mancher glaubt, wir seien zusätzlicher Ballast, fürchtet, dass wir sofort alle Geräte beschlagnahmen, was nicht der Fall ist. Wir sind Partner der Geschädigten, keine Bremsklötze, und können sie aktiv unterstützen. Unser oberstes Ziel ist, im Einvernehmen mit den Unternehmen und IT-Dienstleistern digitale Spuren zu ermitteln.“

Birk betont: „Wenn ein betroffenes Unternehmen sich entscheidet, die Kripo einzuschalten, dann unbedingt unverzüglich! Es handelt sich um einen digitalen Tatort, wir brauchen Spuren! Wenn sich jemand erst nach Tagen meldet, sind die Spuren verwischt.“

IT-Sicherheitsstammtisch: Tipps für den Ernstfall

Weil auch aus Birks Sicht das Thema Cybersicherheit viel zu wenig Aufmerksamkeit in Unternehmen erfährt und vernachlässigt wird, hat er 2024 den IT-Sicherheitsstammtisch ins Leben gerufen. Vierteljährlich sind Interessierte eingeladen, sich bei der Kripo Trier kostenfrei zum Thema zu informieren. „Wir laden externe Experten ein und informieren selbst. Beispielsweise werden Angriffsszenarien durchgespielt. Wir schildern Beispielfälle, geben Tipps und klären auf, was im Ernstfall zu tun ist.“

Wer frühzeitig über den nächsten IT-Sicherheitsstammtisch informiert werden möchte, kann eine Mail an folgende Adresse senden:
kdtrier.ki2.k25@polizei.rlp.de

Cybersicherheit auf einen Blick

Quelle: Horst Schäfer, Geschäftsführer save IT first

Welches sind die größten Risiken für einen Cyberangriff?

1. Der Mensch, das heißt der Mitarbeiter, der aus Mangel an Kenntnissen und Sensibilität unachtsam die IT nutzt und unwissentlich Fehler begeht beziehungsweise Schadsoftware einschleust
2. E-Mail-Kommunikation, insbesondere Phishing-Mails (Mails, bei denen sich hinter dem vermeintlich bekannten Absender ein „Angreifer“ verbirgt)
3. Fehlendes Notfall-Management. Keine klare Festlegung, wer was im Notfall zu tun hat und wer die entsprechenden Ansprechpartner sind
4. Ransomware-Gefahr durch Verschlüsselung der Daten oder Datenklau
5. Mangelhafte technische Ausstattung
6. Mangelhaftes Patchmanagement, das heißt keine ausreichenden Software-Updates, um Schwachstellen zu identifizieren und zu beheben

Wie sollten Unternehmen bei einem Angriff reagieren?

1. **Systeme isolieren:** infizierte Geräte sofort vom Netzwerk trennen, um eine weitere Ausbreitung zu verhindern. Vorhandene Compliance-Regeln und Netzwerksegmentierung sind dabei sehr hilfreich
2. **IT-Verantwortliche informieren:** den IT-Verantwortlichen informieren oder, wenn vorhanden, das Incident-Response-Team (Notfallteam) beziehungsweise den IT-Dienstleister kontaktieren
3. **Beweise speichern:** Logdateien, Screenshots und andere Hinweise für die spätere Analyse speichern
4. **Kein Lösegeld zahlen:** Lösegeld zu bezahlen bedeutet keine Garantie für die Wiederherstellung der Daten
5. **Backup prüfen und wiederherstellen:** saubere und getestete Backups nutzen, um Systeme wiederherzustellen
6. **Forensische Analyse durchführen:** Ursache und Ausmaß des Angriffs ermitteln, um besser vorbereitet zu sein auf einen möglichen nächsten Angriff
7. **Behörden informieren:** bei einem Verstoß gegen die Datenschutzgrundverordnung den Vorfall beim Bundesamt für Sicherheit in der Informationstechnik (BSI) und bei der Polizei melden

Hier gibt es Infos rund um das Thema Cybersicherheit:

IHK Trier: bietet regelmäßig Webinare an. Infos dazu im IHK-Newsletter, *www.ihk-trier.de/newsletter*

Bildungszentrum der IHK Trier: unterschiedliche Seminare, Workshops, Weiterbildungen. Beispielsweise: Weiterbildung zum Cyber Security Advisor (IHK).
8. April bis 22. Mai 2026, Live Online.
weiterbildung.ihk-trier.de

IT-Sicherheitsstammtisch der Kripo Trier, Kommissariat Cybercrime: vierteljährliche Info-Veranstaltung bei der Kripo Trier mit internen wie externen Referenten. Wer über Termine benachrichtigt werden möchte, sollte eine Mail an folgende Adresse schreiben:
kdtrier.ki2.k25@polizei.rlp.de