IT-Sicherheit: Die Wirtschaft im Fokus der Cyberkriminalität

Die Angriffswelle der Hacker rollt – permanent

Nehmen die Unternehmen die IT-Sicherheit ernst genug? Jüngste Vorfälle und die akute Bedrohungslage zeigen die Priorität.

Von Michael Ertel

Akut und permament bedroht: die IT-Infrastruktur in den Unternehmen. *Foto: Gorodenkoff /Adobe Stock*

Oberfranken – Erpressung, Sabotage, Produktionsausfälle, Ideen- und Patentdiebstahl – und letztendlich ein erheblicher finanzieller Schaden und eine angekratzte Reputation. Die Risiken für die Unternehmen durch Cyberattacken steigen. Dies zeigt der kürzlich veröffentlichte „Lagebericht 2018“ des Bundesamtes für Sicherheit in der Informationstechnik (BSI): Knapp 70 Prozent der Unternehmen und Institutionen in Deutschland seien 2016 und 2017 Opfer von Angriffen geworden. Und dies, obwohl „die IT-Sicherheit eine unabdingbare Voraussetzung einer erfolgreichen Digitalisierung ist“.

Wie aus der potenziellen Gefahr ein reales Angriffsszenario wird, musste vor wenigen Wochen der Maschinen- und Anlagenbauer Krauss-Maffei an seinem Hauptsitz in München erkennen. Ein Verschlüsselungstrojaner, sogenannte Ransomware, versperrte Zugriffe auf Rechner und Dateien – verbunden mit einer hohen Lösegeldforderung. Besonders hart traf es den Produktionsbereich: Computergesteuerte, automatisierte Fertigungs- und Montageanlagen waren völlig lahmgelegt.

Aber auch weniger prominente Firmen geraten in das Fadenkreuz der Hacker. Die „Hidden Champions“ in Oberfranken sieht der Hofer IT-Sicherheitsberater Friedrich Schraml ebenso gefährdet. „Wir haben hier viele Marktführer mit innovativen Ideen und spezialisierten Marktsegmenten. Sie sind besonders exponiert und müssen natürlich auch damit rechnen, in den Fokus zu geraten.“

Schraml kennt die IT-Welt und hat alle Phasen der „digitalen Revolution“ in seiner 40-jährigen Berufstätigkeit erlebt: Viele Jahre war er in einem internationalen Konzern IT-Manager. 2017 hat er sich als Datenschutzauditor und Berater für IT-Sicherheit selbständig gemacht. Seine Klientel sind nun mittelständische Unternehmen, die sich zum einen an den Regelungen der Datenschutzgrundverordnung (DSGVO) abkämpfen, zum anderen ihre IT gegen Angriffe schützen wollen.

Was Friedrich Schraml betont: Sind die Hacker durch Phishing-Methoden, also dem Abschöpfen von Passwörtern, erst einmal in die Firmennetzwerke eingedrungen, geht es ihnen weniger um Industriespionage und das Ausspähen von Firmengeheimnissen, als vielmehr um pure Erpressung. „Das sind tatsächlich klassische Bösewichter, die mit höchster krimineller Energie die Systeme sperren und für deren Freigabe horrende Lösegelder fordern.“ Das recht einfache Grundprinzip, Mitarbeiter in den Unternehmen durch Links in E-Mails auf täuschend echt aussehende, aber gefälschte Anmeldeseiten im Internet zu leiten und dort ihre Passwörter abzugreifen, funktioniere nach wie vor – trotz aller Warnungen. „Wenn diese Tür in die IT-Infrastruktur erst einmal durchschritten ist, öffnet sich den Hackern eine große Welt, in der sie sich völlig frei bewegen können.“

„Wichtig sind mitdenkende Mitarbeiter.“
Melanie Wächter, Projektleiterin Firma Procomp

Natürlich gibt es dagegen technologiegestützten Schutz. Und diesen nicht nur von internationalen Securityfirmen, sondern auch von regionalen Anbietern. Das Marktredwitzer Systemhaus Procomp automatisiert mit sogenannten „Managed Services“ die Echtzeitüberwachung der IT-Infrastruktur. „Wir sind an die Systeme unserer Kunden direkt angebunden und überwachen, ob Angriffe stattfinden und an welchen Stellen“, erklärt Melanie Wächter, Projektleiterin im Vertrieb. Darüber hinaus analysiere man präventiv die Systeme der Kunden und schließe Sicherheitslücken auf den Servern und bei den Clients, also den Computern der Mitarbeiter. „Außerdem standardisieren wir das Patch-Management, sodass alle Windows-Updates automatisch installiert und die Betriebssysteme auf dem aktuellsten Stand gehalten werden.“

Dennoch: Eine hundertprozentige Sicherheit garantieren auch diese „True Detection-Systeme“ nicht. „Natürlich gibt es viele technische Lösungen für die IT-Sicherheit“, unterstreicht Friedrich Schraml. Doch selbst eine Firewall könne Phishing-Mails, die ja selbst noch keinen Virus enthalten, nicht aufhalten. „Wichtig sind mitdenkende Mitarbeiter, die man vorher entsprechend sensibilisiert hat“, betont auch Melanie Wächter. Das heißt: Die Lücken in der IT-Sicherheit reißen meist die Menschen in den Unternehmen. Um sie im Umgang mit den immer trickreicher und intelligenter werdenden Spams zu schulen, schickt ihnen das Security-System von Procomp in gewissen Abständen elektronische Post. Wird diese von den Mitarbeitern nicht als Spam erkannt und geöffnet, erhalten sie automatisiert die Einladung zu einer Schulung.

Und in vielen Unternehmen „schlummert“ noch ein weiteres Sicherheitsrisiko: veraltete Rechner. Computer, die noch mit Windows-XP-Betriebssystem laufen, sind keine Seltenheit – insbesondere in Produktionsbereichen als Steuerungskomponente von Maschinen. „Solche PCs lassen sich nicht mehr durch Updates sicher machen“, ist IT-Experte Schraml überzeugt. Sie seien ein Einfallstor für Schadsoftware, vor allem dann, wenn sie für Fernwartungszwecke mit dem Internet verbunden seien. „Hier hilft nur eins: sofort vom Netz nehmen.“

Trotz dieser akuten Bedrohungslage sieht die Zentralstelle Cybercrime Bayern (ZCB) viele Firmen nur unzureichend gewappnet. Die Verantwortlichen investierten aus Kostengründen nicht genügend in die Cybersecurity, meint der Generalstaatsanwalt und ZCB-Leiter Thomas Janovsky. Seit Anfang 2015 bearbeitet seine Behörde bayernweit Verfahren gegen Internetkriminalität. Nun stellt er fest: „Man spart, was Software-Updates betrifft, und wundert sich dann, wenn plötzlich die ganze IT stillsteht.“

„An dem Denken, dass die Cyber-Sicherheit vor allem Geld kostet, hat sich leider noch nicht überall etwas geändert“, bemerkt auch Friedrich Schraml. In vielen mittelständischen Unternehmen fehlten die Experten im Hause. „Die Alternative sind externe Spezialisten. Aber auch die will man nicht einkaufen.“

„Die Schwachstelle sind die Mitarbeiter“

Die Cyber-Risiken steigen: Der IT-Professor Dr. Torsten Eymann fordert von den Unternehmen eine „langfristige Orientierung“ bei Investitionen in die Sicherheit.

Herr Dr. Eymann, deutsche Unternehmen schätzen Hackerangriffe als eines der größten Risiken ein. Was überwiegt: Sabotage oder Spionage?

Das hängt davon ab, welche Personen mit welchen Interessen agieren. Früher hatten wir es mit Hackerangriffen von Leuten zu tun, die es einfach mal ausprobiert haben. Einfach Skripte aus dem Internet runterladen und los geht's. Das ist aber nicht professionelle Industriespionage. Diese geschieht meist direkt in den Unternehmen durch Mitarbeiter, die die Firma verlassen und dann Daten mitnehmen. Das heißt: Angriffe von außen auf die IT mit dem Ziel der Industriespionage sind – gerade im Mittelstand – eher die Seltenheit.

Und durch welche Angriffe ist die IT der Unternehmen dann tatsächlich bedroht?

Eindeutig durch Ransomware, also die Verschlüsselung von Systemzugriffen und Dateien verbunden mit einer Lösegeldforderung. Denn dahinter steckt bei den Angreifern erstmals ein echtes Geschäftsmodell. Und zwar eines, das sehr einfach zu verstehen und durchzuführen ist. Man kann sich im Darknet Skripte kaufen, die das machen. Und eine Bitcoin-Adresse für das Lösegeld kann anonym erstellt werden. Das probieren viele Hacker aus. Sie müssen lediglich das Gefühl haben, dass bei der attackierten Firma auch etwas zu holen ist, dass es also ein Unternehmen mit Wert ist. Der Reiz ist somit die Gelderpressung – denn allein von der Sabotage einer IT-Infrastruktur profitieren die Kriminellen ja nicht.

Der Digitalverband Bitkom geht davon aus, dass in den vergangenen zwei Jahren 68 Prozent der deutschen Unternehmen Opfer von Cyberattacken wurden; die Angriffe seien mittlerweile „alltägliche Realität“. Das klingt alarmierend.

Sicherlich. Aber man muss ja differenzieren, dass nicht jede Spam-Mail-Attacke, die man als Angriff werten kann, die Hacker zum Erfolg führt. Viele Zahlen, die hier im Umlauf sind, sind durch eine gewisse Hysterie in den Medien geprägt. Auch an unserer Universität stellen wir zwar horrende Zahlen fest, meist verursacht durch automatisch ablaufende Skripte gegen E-Mail- und Webserver. Aber in vielen Fällen sind das noch keine tatsächlichen Angriffe.

Das heißt: Es wird zu wenig zwischen Attacke und tatsächlich erfolgreichem Angriff unterschieden?

Man muss einfach zwischen Schwachstelle, Bedrohung und Angriff differenzieren. Natürlich ist es potenziell gefährlich, wenn versucht wird, mit einer fingierten Rechnung oder Bewerbung über ein PDF-Dokument einen Verschlüsselungstrojaner einzuschleusen. Aber die große Schwachstelle bei solchen gezielten Angriffen sind eben Mitarbeiter, die leichtfertig agieren und diese Dateien öffnen. Die Menschen in den Unternehmen bieten noch immer das größte Einfallstor für Viren und Schadsoftware – oft ganz unbewusst beim täglichen Arbeiten. Personal, Einkauf, Versand und Logistik sind hier die prädestinierten Bereiche, da man dort viele digitale Unterlagen, die als Arbeitsgrundlage dienen, zugeschickt bekommt.

Neben den technischen Lösungen sehen Sie somit den „Faktor Mensch“ als entscheidend für die IT-Security?

Es geht tatsächlich um eine bessere Sensibilisierung von Personen. Die Universität Bayreuth befindet sich in einer ähnlichen Situation wie ein mittelständisches Unternehmen. Um ein größeres Bewusstsein für die IT-Sicherheit zu wecken, finden bei uns zweimal im Jahr Schulungen mit einem Live-Hacking statt. Außerdem gibt es noch ein zusätzliches Seminar explizit zur E-Mail-Sicherheit. Seitdem wir das machen, wird wesentlich seltener auf verdächtige Links oder PDF-Dateien geklickt.

Interview

mit Dr. Torsten Eymann, Professor für Betriebswirtschaftslehre

Und der Mensch spielt sicherlich ebenso eine Rolle als wichtige Ressource bei der Gefahrenabwehr, also in den IT-Abteilungen? Doch auch die Bamberger Zentralstelle Cybercrime bemängelt, dass in vielen Unternehmen bei der IT-Sicherheit – und damit an der falschen Stelle – gespart werde.

Das Problem ist: Man möchte genau so viel in die IT-Sicherheit investieren, dass man zwar alle möglichen Dinge abwehren kann, aber trotzdem nicht zu viel Geld ausgibt. Die Frage ist also: Wie viele IT-Sicherheitsmitarbeiter braucht man? Zwei, vier oder zehn? Man kann das nur ganz schwer beziffern. Denn auf der anderen Seite ist ja nicht klar, wie hoch der Schaden wäre. Somit fällt eine betriebswirtschaftliche Aussage, wie viele Leute man beschäftigen soll oder wie teuer eine Firewall sein darf, schwer. Werden Vorfälle, wie kürzlich die Ransomware-Attacke bei Krauss-Maffei, publik, dann steigt zwar die Ausgabebereitschaft kurzfristig an. Aber bei der IT-Sicherheit braucht man eine langfristige Orientierung. Da hilft ein Vergleich mit Feuerwehr und Katastrophenschutz: Wie wichtig diese Dinge sind, merkt man meist erst, wenn etwas passiert ist.

Aber bei einem Produktionsausfall kann man doch genau beziffern, was dieser kostet?

Das ist richtig. Dort, wo man auf Basis einer gewissen Eintrittswahrscheinlichkeit einen Vorfall lokalisieren kann, ist es auch möglich, den Schaden zu berechnen und sich mit Cyberpolicen sogar zu versichern. Dennoch braucht man Mitarbeiter, die sich ständig mit dem Thema auseinandersetzen – am besten mit einer unbegrenzten Perspektive.

Industrie 4.0 und vernetzte Produktionen werden zunehmend real. Auch Entwicklungskooperationen zwischen Unternehmen laufen über digitale Plattformen oder gar Zugriffe in die IT-Struktur des jeweils anderen. Wird sich dadurch das Sicherheitsrisiko noch weiter erhöhen?

Ein zusätzliches Gefahrenpotenzial ergibt sich immer bei neuen Dingen. Wenn sich Werkstücke selbst den Weg durch die Fertigung suchen oder Produktionssysteme autonom arbeiten, dann kreiert das auch neue Sicherheitsrisiken. Insbesondere dann, wenn Maschinensteuerungen für das Internet geöffnet werden müssen. Aber es gibt ja auch Zertifizierungen und Prüfungen von Sicherheitslevels. In der Automobilindustrie setzt man auf die Standardreihe ISO 27 000, die bereits jetzt eine wichtige Grundlage für Entwicklungspartnerschaften ist. Die Chance dabei ist: Wer diesen IT-Sicherheitsrahmen strikt einhält und dafür Geld investiert, ist als lokaler Partner in Deutschland vertrauenswürdiger als irgendeine Firma aus Fernost. So finden möglicherweise viele Leistungen, die derzeit noch Offshore erbracht werden, wieder ihren Weg zurück zu uns.

Foto: Universität Bayreuth
Das Gespräch führte Michael Ertel

Zur Person

Prof. Dr. Torsten Eymann hat an der Universität Bayreuth seit 2004 den Lehrstuhl für Betriebswirtschaftslehre inne, insbesondere Wirtschaftsinformatik. Zudem ist er stellvertretender Leiter der Projektgruppe Wirtschaftsinformatik des Fraunhofer FIT. Von 2009 bis 2015 war er Präsident des Betriebswirtschaftlichen Forschungsinstitutes für Fragen der mittelständischen Wirtschaft an der Universität Bayreuth e. V. (BF/M).

Kyocera kauft H.C. Starck Ceramics

Selb – H.C. Starck verkauft die Tochtergesellschaft H.C. Starck Ceramics mit Sitz in Selb an den japanischen Technologiekonzern Kyocera. Wie das Unternehmen mitteilt, haben beide Partner eine entsprechende Vereinbarung unterzeichnet. Beide Firmen rechnen damit, den Verkauf im ersten Halbjahr abzuschließen. Die Arbeitsverhältnisse aller aktuell rund 200 Mitarbeiter bleiben demnach bestehen.

„Wir freuen uns außerordentlich, mit Kyocera den idealen Partner für die Division Ceramics gefunden zu haben“, wird Dr. Jens Knöll, Geschäftsführer der H.C. Starck GmbH, zitiert. „Das Interesse Kyoceras bestätigt die erfolgreiche Wachstumsstrategie der Division.“

Die Kyocera Corporation mit Hauptsitz in Kyoto ist ein Anbieter feinkeramischer Komponenten für die Technologieindustrie. Im Geschäftsjahr 2018 verzeichnete Kyocera einen Umsatz von konsolidiert etwa zwölf Milliarden Euro.

H.C. Starck Ceramics produziert in Selb hochpräzise Großbauteile für die Halbleiterindustrie und stellt Pulver und Bauteile aus technischer Keramik her. In den vergangenen Jahren hat die H.C. Starck Ceramics laut Mitteilung das Produktportfolio gewechselt. Ende 2017 wurde eine neue Werkhalle mit einer Fläche von 2000 Quadratmetern in Betrieb genommen. Für das laufende Jahr ist eine nochmalige Erweiterung der Produktionsflächen geplant.

Bereits im März vergangenen Jahres hatte die „Frankfurter Allgemeine Zeitung“ unter dem Titel „H.C. Starck wird weiter zerteilt“ über eine Aufspaltung des ehemaligen Bayer-Konzernteils berichtet. Damals hatten die Sprecher der Eigentümer, Advent International und The Carlyle Group, auf Nachfrage unserer Zeitung zu einem Verkauf der H.C. Starck GmbH mitgeteilt, „derartige Spekulationen grundsätzlich nicht zu kommentieren“. *red*

Digitale Infrastruktur hinkt weit hinterher

München – BMW-Chef Harald Krüger hat einen schnelleren Ausbau der digitalen Infrastruktur in Deutschland angemahnt. Es mache ihm „Sorgen, wie langsam wir in Deutschland sind“, sagte Krüger in einem Interview der „Passauer Neuen Presse“ und des „Donaukurier“. „Wir müssen die Chancen der Digitalisierung endlich gestalten.“ Nötig sei eine 5G-Mobilfunk-Infrastruktur für automatisiertes Fahren – und das nicht nur in Metropolen.

Beim Thema autonomes Fahren bremse die Bürokratie die Technologie aus, sagte Krüger weiter. Dies betreffe den Fahrzeugzulassungsprozesses bis hin zur Haftung und der Frage des Datenaustausches. Alles dies müsse zügig geklärt werden. „Ich bin viel in China unterwegs und kann nur sagen: China schafft in all diesen Zukunftsthemen in unglaublicher Geschwindigkeit machtvolle Tatsachen.“ *dpa*

Winzer ernten wegen Dürre weniger

Naumburg – Qualität statt Quantität: Winzer der Saale-Unstrut-Region haben für das wärmste und trockenste Weinjahr seit Beginn der Aufzeichnungen Bilanz gezogen. 2018 sei eine Erntemenge von 4,64 Millionen Litern erreicht worden – deutlich weniger als in den Jahren zuvor, teilt der Weinbauverband Saale-Unstrut anlässlich seiner Generalversammlung mit. Den deutlichen Einbußen aufgrund des Wetters stünden jedoch teils sehr hohe Qualitäten gegenüber. So seien besonders gehaltvolle, aromatische Weißweine und kraftvolle Rotweine in die Flaschen gekommen, hieß es.

2018 sei mit einem sehr frühen Start der Lese im August und deren Abschluss im Oktober ein „Weinjahr der Superlative“ gewesen. Die Reben hätten sich gesund präsentiert, seien aber im Trockenstress gewesen. Schäden durch Spätfröste, Hagel oder Erosion seien nicht bekannt. *dpa*