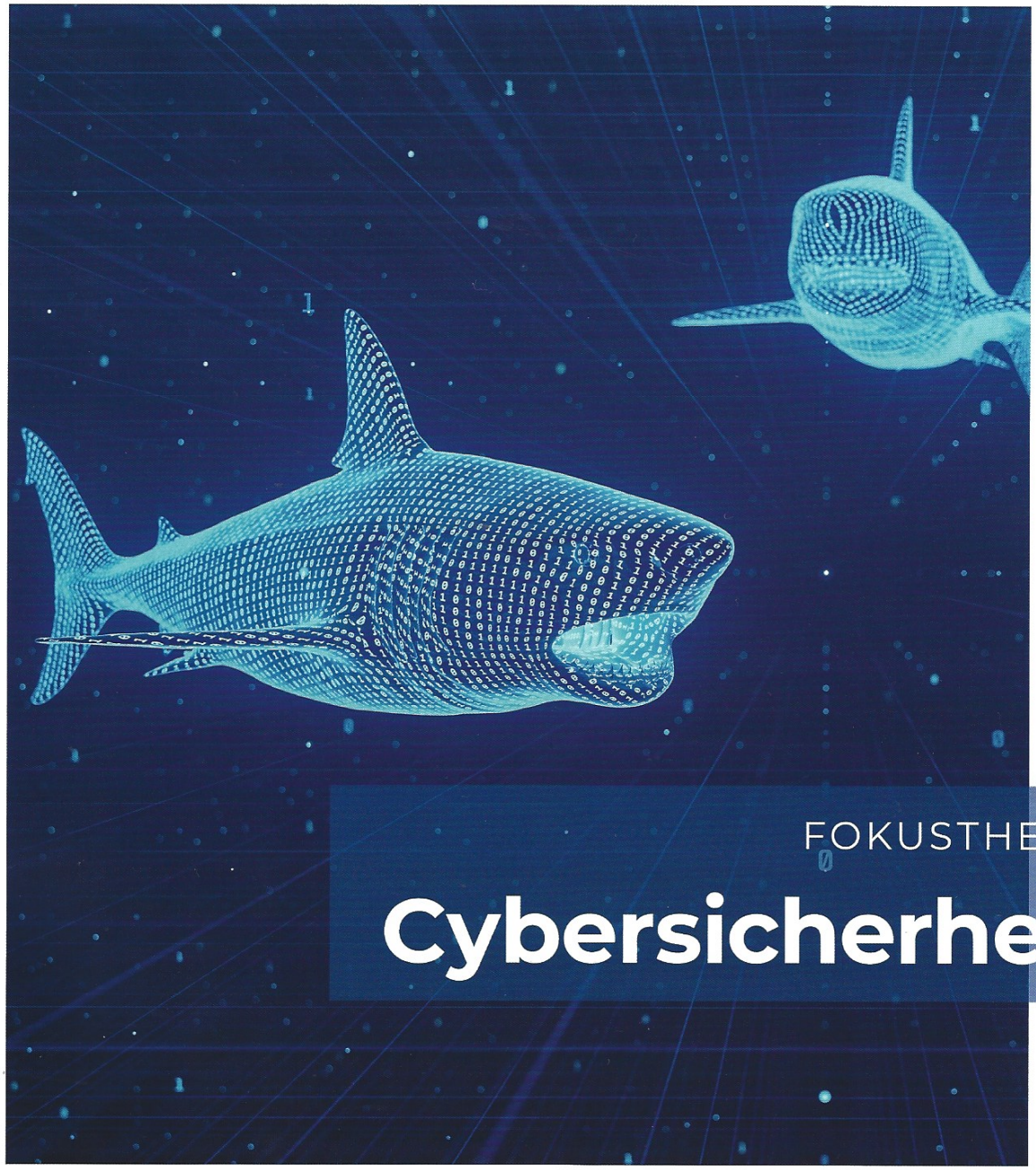
IHK Industrie- und Handelskammer Frankfurt am Main

02|03.2023

IHK WirtschaftsFORUM

Ihr Unternehmermagazin für die Region FrankfurtRheinMain

A 4836 | Jahrgang 146



FOKUSTHEMA

Cybersicherheit

www.frankfurt-main.ihk.de

Foto: istock / Hwangdaesung

FOKUSTHEMA

Cybersicherheit

CYBERANGRIFFE

Ein lukratives Geschäftsmodell

Infolge zunehmender Digitalisierung und globaler Vernetzung sind Unternehmen aller Größen und Branchen mehr denn je im Visier von Hackern. Denn Cyberattacken sind für Internetkriminelle vor allem eines: ein florierendes Geschäftsmodell.

Ausgerechnet Weihnachten. Eigentlich versetzen die umsatzstärksten Monate die deutschen Elektronikhändler alle Jahre wieder in Festtagsstimmung. Handys, Fernseher, Laptops rangieren schließlich auf den Wunschlisten von Groß und Klein weit vorn. Doch dann griffen Hacker mit einem Verschlüsselungstrojaner die Server eines Handelsunternehmens an, der Ransomware-Angriff legte Teile des Warenwirtschaftssystems und der Kassen lahm. Kunden konnten zwar weiterhin einkaufen, aber weder Waren bestellen noch abholen oder zurückgeben. Rund 1000 Märkte in Europa waren betroffen, mehr als 400 allein in Deutschland. Ursprünglich hatten die Datendiebe 240 Millionen US-Dollar Lösegeld gefordert, senkten die Summe dann aber auf 50 Millionen.

„Kein Back-up, kein Mitleid“

Nach Fällen wie diesem müssen die Autoren des Jahresberichts zur Lage der IT-Sicherheit in Deutschland nicht lange suchen. „Nie war die Gefahr, durch einen Cyberangriff aus dem Markt gedrängt oder empfindlich geschädigt zu werden, größer als heute“, warnt Manuel Bach, Leiter des Referats „Cyber-Sicherheit für Kleine und Mittlere Unternehmen“ im Bundesamt für Sicherheit in der Informationstechnik (BSI). Gleichzeitig fehle es an IT-Dienstleistern, die Unternehmen gegen die Attacken verteidigen könnten. Das BSI warnt vor einem grundsätzlichen Engpass beim Personal für den Umgang mit IT-Sicherheitsvorfällen.

Erpressung als Geschäftsmodell

Praktisch jedes Unternehmen in Deutschland wird Opfer. 84 Prozent waren im Jahr 2022 betroffen, weitere neun Prozent gingen davon aus. „Inzwischen sollte jedem klar sein, dass die große Mehrheit der Cybervorfälle und -katastrophen schlicht und ergreifend Zufallstreffer oder Kollateralschäden sind, denn die meisten Angriffe werden nicht gezielt auf einzelne Unternehmen ausgeführt, sondern sind eher ein breites Geschäftsmodell der modernen Erpressung“, warnt Markus J. Krauss, Head of Cisco Cloud Security bei Cisco Systems, Eschborn. Den Schaden durch Diebstahl von IT-Ausrüstung und Daten, Spionage und Sabotage bezifferte der Digitalverband Bitkom in 2022 auf rund 203 Milliarden Euro. Sprunghaft gestiegen sind laut Studie zuletzt die Angriffe aus China und Russland. 43 Prozent der Befragten identifizierten mindestens eine Attacke aus China, 36 Prozent machten einen Urheber aus Russland aus.

IHK ONLINE

Ausführliche Infos zum Thema Cybersicherheit in Unternehmen finden Sie auf den Internetseiten des Bundesamts für Sicherheit in der Informationstechnik (BSI):

www.bsi.bund.de

Wenig beruhigend auch: Die Angreifer gehen immer professioneller vor. Jeder zweite Täter kommt aus dem organisierten Verbrechen. 2021 lag deren Anteil gerade mal bei 29 Prozent. Bitkom-Präsident Achim Berg beobachtet: „Spätestens mit dem russischen Angriffskrieg gegen die Ukraine und einer hybriden Kriegsführung auch im digitalen Raum ist die Bedrohung für die Wirtschaft in den Fokus von Unternehmen und Politik gerückt." Aber auch der massive Digitalisierungsschub seit Beginn der Coronapandemie ließ die digitalen Angriffe hochschnellen.

Foto: Amin Akhtar

Andreas Schmidt, Leiter des Referats IT und Geheimschutz, Bundespräsidialamt: „Beim Thema Cybersicherheit sucht man wirklich gut aufgestellte Unternehmen leider häufig noch vergebens."

Jedes Unternehmen ist gefährdet

Andreas Schmidt leitet beim Bundespräsidialamt das Referat IT und Geheimschutz und ist dessen IT-Sicherheitsbeauftragter. Als ISO-27001-Auditor und IS-Revisor führt er darüber hinaus bei Unternehmen Audits und Revisionen unter anderem nach der Methodik des IT-Grundschutzes des BSI durch. Für ihn gibt es drei Gruppen: Unternehmen, die auf gut Glück hoffen, dass nichts passiert, und deshalb noch gar nicht systematisch an das Thema herangegangen sind. Eine zweite Gruppe muss handeln, weil ein Vorstand oder ein bedeutender Kunde dies einfordert. Sie weiß aber gar nicht, wie sie das Thema überhaupt angehen soll. Die dritte Gruppe ist gesetzlich verpflichtet, bestimmte Sicherheitsmaßnahmen einzuhalten. Aktuell sind vor allem die Betreiber Kritischer Infrastrukturen (Kritis) betroffen. „Anfangs gehörten zu dem Kreis zum Beispiel die Energieversorger, heute sind es aber auch schon deren Zulieferer", so Schmidt. In der geplanten dritten Fassung des IT-Sicherheitsgesetzes werde das Bundesinnenministerium diese Gruppe sicher noch einmal stärker ausweiten. Schmidts Fazit: „Beim Thema Cybersicherheit sucht man wirklich gut aufgestellte Unternehmen leider häufig noch vergebens. Der große Druck kommt, wenn der erste Sicherheitsvorfall stattgefunden hat."

Auch Experte Bach vom BSI beobachtet: „Der größte Irrtum ist, dass viele mittelständische Unternehmen glauben, sie seien zu klein, um ein lohnendes Ziel für einen Angriff darzustellen. Sie sind

Nützliche Links

Kleine und mittlere Unternehmen (KMU) werden zunehmend Ziel von Cyberattacken. Nicht selten führen diese zu immensen Schäden, bis hin zur Existenzbedrohung, und schwächen die Unternehmensreputation. Auf der BSI-Homepage finden Sie ausgewählte Tipps für Firmen ohne IT-Expertise und für Unternehmen, die sich bereits eigene oder extern beauftragte IT-Fachleute leisten.

Erste Hilfe bei IT-Sicherheitsvorfällen

Auch wenn die Gefahr von Cyberattacken hinlänglich bekannt ist, trifft es viele Unternehmen dann doch überraschend. Was bei einem IT-Sicherheitsvorfall organisatorisch, rechtlich und technisch zu beachten ist, erfahren Sie hier:

deshalb nicht adäquat geschützt." Dabei könnten auch kleine und mittelgroße Unternehmen (KMU) mit begrenzten personellen und finanziellen Ressourcen mit kostengünstigen Maßnahmen und Vorsorge Angriffe abwehren und den Schaden begrenzen. „Für einen Vorstand oder Geschäftsführer gehört das Thema deshalb längst ganz oben auf die tägliche Agenda", unterstreicht Krauss von Cisco.

Eine signifikante Bedrohung

Wie groß der Schaden sein kann, weiß die Wirtschaftsprüfungs- und Beratungsgesellschaft PwC. 88 Prozent der befragten deutschen Unternehmen waren in den vergangenen drei Jahren Opfer einer Cyberattacke, die mindestens 10000 Euro Schaden verursacht hat. Bei knapp jedem dritten Attackierten waren es unter 100000 Euro, bei 26 Prozent jedoch zwischen 100000 und einer Million Euro und bei 30 Prozent sogar mehr als eine Million Euro, heißt es in der Studie „Global Digital Trust Insights 2023". Zwei Drittel der Befragten erachteten Cyberkriminelle als die signifikanteste Bedrohung für ihre Organisation. Danach folgten Hacker (42 Prozent), Wettbewerber (39 Prozent) sowie aktuelle, ehemalige und freie Beschäftigte (36 Prozent). Zu den häufigsten erwarteten Einfallstoren zählen E-Mails (46 Prozent), mobile Endgeräte (44 Prozent) und cloudbasierte Angriffsvektoren (34 Prozent).

Sicherheitstechnologie oft veraltet

Eine aktuelle Cisco-Studie kommt zu dem Schluss: Lediglich 20 Prozent der Entscheider für IT-Sicherheit in Deutschland sind davon überzeugt, die gravierendsten Risiken bewältigen und größere Vorfälle vermeiden zu können. Und 48 Prozent sagen, dass die Sicherheitstechnologien in ihrem Unternehmen veraltet sind. Doch das ist nur der eine, technologische Teil des Gesamtproblems. Dr. Alexander Köppen, Partner bei PwC Deutschland im Bereich Cyber Security and Privacy, beobachtet, dass „viele Unternehmen ihre Cyberstrategie auf Leitungsebene noch gar nicht definiert haben". Zunächst müsse deshalb aus Geschäftsmodell, regulatorischen Anforderungen, Bedrohungslage und Risikobereitschaft ein spezifischer Ansatz hergeleitet werden. In

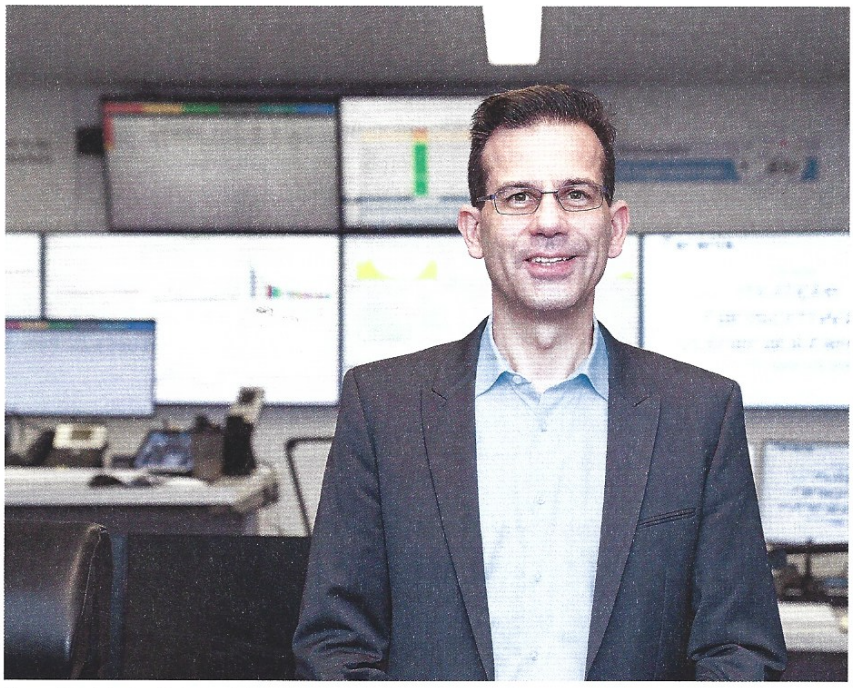


Foto: BSI

Manuel Bach, Leiter, Referat „Cyber-Sicherheit für Kleine und Mittlere Unternehmen", BSI: „Nie war die Gefahr, durch einen Cyberangriff aus dem Markt gedrängt oder empfindlich geschädigt zu werden, größer als heute."

CHECKLISTE

Eine BSI-Checkliste informiert über die wichtigsten Basiselemente der IT-Sicherheit:

- Updates: Halten Sie Ihre Software durch Sicherheits-Updates auf dem neuesten Stand.
- Passwörter: Verwenden Sie starke und unterschiedliche Passwörter. Hierfür können Sie einen Passwortmanager nutzen.
- Zwei-Faktor-Authentisierung: Neben dem ersten Faktor (meist Passwort) nutzen Sie in einem zweiten Schritt zum Beispiel Ihren Fingerabdruck oder eine TAN.
- Virenschutz: Antivirenprogramme überprüfen den gesamten Rechner auf Anzeichen einer Infektion. Updates nicht vergessen.
- Firewall: Sie schützt vor Angriffen von außen und verhindert, dass schädliche Programme Kontakt vom Gerät zum Internet aufnehmen.
- Backup: Ohne vorhandene und lesbare Datensicherung können im Zweifelsfall keine Daten wiederhergestellt werden.

Quelle: Bundesamt für Sicherheit in der Informationstechnik (BSI)

einem zweiten Schritt geht es um die Regelung der Governance. „Wer hat welche Verantwortlichkeiten und wie sind diese über die Unternehmensgruppe verteilt, etwa zentral oder dezentral." Darüber hinaus müssten Cyberrisiken auch quantifiziert werden.

„Die wenigsten Unternehmen haben eine Antwort darauf, welchen finanziellen Schaden Cyberrisiken anrichten können. Und um welche Höhe sie das Risiko mit entsprechenden Investitionen minimieren können." Von den organisatorischen Maßnahmen müssten die Unternehmen deshalb auch zu einer Effektivitätsmessung kommen. Dabei helfen neben Reporting und Audits technische Maßnahmen wie Pentesting. Unabhängige Sicherheitsanalysten untersuchen dabei die IT auf Sicherheitslücken und Verwundbarkeiten. Zu gängigen IT-Security-Übungen zählen zudem der Einsatz von roten Teams, sogenannten Red Teams, die IT-Angriffe simulieren, und Blue Teams, die die Aufgabe der Verteidiger übernehmen.

Foto: Goetzke Photographie

Markus J. Krauss, Head of Cisco Cloud Security, Cisco Systems: „Die meisten Angriffe werden nicht gezielt auf einzelne Unternehmen ausgeführt, sondern sind eher ein breites Geschäftsmodell der modernen Erpressung."

Faktor Mensch

Oft ist es nicht einmal ausgeklügelte Technik, die den Kriminellen das Tor zum Datenschatz eines Unternehmens öffnet. Für Cisco-Manager Krauss ist der Faktor Mensch immer das schwächste Glied in der Kette. Beim Phishing (Fischen nach Passwörtern), der bekanntesten Form des sogenannten Social Engineering, nutzen Betrüger die Gutmütigkeit oder Hilfsbereitschaft ihrer Opfer aus, indem sie versuchen, deren Vertrauen zu gewinnen. Telefonisch melden sich zum Beispiel angebliche Microsoft-Mitarbeiter, die in gebrochenem Englisch behaupten, dass der Rechner von Viren befallen sei. Sie bie-

Broschüre „Cyber-Sicherheit für KMU"

Das BSI bietet mit der Broschüre „Cyber-Sicherheit für KMU" vor allem kleinen und mittelständischen Unternehmen einen leicht verständlichen Einstieg, um das Cyber-Sicherheitsniveau zu verbessern. Sie informiert unter anderem darüber, wer für die Informationssicherheit im Unternehmen verantwortlich ist, warum Patches und Updates regelmäßig installiert werden sollten, warum ein Virenschutzprogramm notwendig und eine Datensicherung so wichtig ist. **www.bsi.bund.de** Cyber-Sicherheit für KMU

DREI FRAGEN AN

Professor Kristina Sinemus, hessische Ministerin für digitale Strategie und Entwicklung, über das Programm Distral (Eigenschreibweise Distr@l), das anwendungsorientierte Lösungen für die Cybersicherheit von Unternehmen fördert

Frau Ministerin, warum geraten verstärkt kleine und mittelständische Unternehmen ins Visier von Hackern?
Durch den Digitalisierungsschub geraten vor allem KMU zunehmend ins Visier von Cyberangriffen, da diese im Vergleich zu größeren Unternehmen häufig über schwächere Sicherheitssysteme und ein geringeres IT-Budget verfügen.

Deshalb haben Sie jüngst die Förderung von Schutzmaßnahmen vor Cyberangriffen in das Digitalisierungsprogramm Distral aufgenommen?
Um KMU zukunftssicher aufzustellen, wurde die Förderung von neuen Lösungen vor Hacker- und IT-Angriffen in Hessens größtem Programm im Bereich Digitalisierung, Distral, aufgenommen. Damit werden gezielt und in Deutschland einmalig anwendungsorientierte Lösungen für die Cybersicherheit von KMU in Hessen gefördert.

Welche Investitionen von KMU in die Cybersicherheit können gefördert werden?
Vor allem die Entwicklung neuer Programme und Verfahren zum Scannen von Schwachstellen und die Weiterentwicklung bestehender Softwarelösungen.

Die Fragen stellte Petra Menke, IHK Frankfurt.

ten ihre schnelle Hilfe an und bitten um Passwörter.

Ausgefuchste Datendiebe gehen noch einen Schritt weiter und profitieren letztlich von leicht gemachter Recherche in sozialen Medien. Schnell findet sich dort der Name des IT-Verantwortlichen oder CEO eines Unternehmens. Mit dessen Namen meldet sich ein Betrüger bei einem Mitarbeiter und fragt nach einem Passwort. Oder ein CEO fordert per Mail seinen Finanzer auf, umgehend eine Summe x für einen Notfall zu überweisen, weil sonst ein großer Auftrag verloren gehe. Selbst mit der Materie Vertraute sind schon schwach geworden, weil sie in solch einer Situation nicht genau wissen, ob die Geschichte wahr oder erlogen ist.

Nutzerrechte überprüfen

Kontinuierliche Schulungen sind deshalb unerlässlich, um das Bewusstsein der Mitarbeiter zu schärfen. Schmidt vom Bundespräsidialamt fällt bei seinen Audits zudem auf, wie fahrlässig viele Unternehmen mit der IT-Sicherheit umgehen. Ein Beispiel: Der Azubi, der verschiedene Stationen durchläuft, hat die meisten Nutzerrechte von allen und wird wie ein Topmanager behandelt. „Das haben die meisten gar nicht auf dem Schirm", moniert Schmidt. Wichtig sei es auch, Meldeketten zu etablieren, damit im Fall eines Angriffs schnell reagiert werden kann. Im Idealfall werde der GAU regelmäßig geübt. Wenn ein Mitarbeiter berichtet, dass etwas Komisches auf seinem Bildschirm passiert, wie muss dann wer reagieren? Schmidt: „Die Entscheidungen, was im Notfall zu tun ist, werden häufig viel zu spät getroffen."

„Kein Back-up, kein Mitleid": Für Unternehmer, die bei der technischen IT-Sicherheit die grundlegenden Standards nicht befolgen, haben Dr. Michael Kreutzer und Thomas Dexheimer kein Verständnis. Die beiden Forscher arbeiten am Nationalen Forschungszentrum für

Foto: Fraunhofer SIT

Dr. Michael Kreutzer (l.) und Thomas Dexheimer (r.), Forscher im Nationalen Forschungszentrum für angewandte Cybersicherheit Athene: „Wenn Produktionssysteme angegriffen werden, kann eine Cyberattacke bis zur Insolvenz führen."

angewandte Cybersicherheit Athene, einer Einrichtung der Fraunhofer-Gesellschaft, das zu den weltweit führenden Forschungsinstituten für Cybersicherheit und Privatsphärenschutz zählt. Laut Kreutzer müssen die Sicherungskopien verschlüsselt sein, an einem anderen physikalischen Ort als die operativen Systeme liegen und die gesicherten Daten dürfen nicht überschrieben werden können. Zugleich sollen sie wieder leicht einspielbar sein. „Dazu müssen die Verantwortlichen wissen, wo genau alle Daten liegen und ob diese vom Backup tatsächlich erfasst werden."

Newsletter für KMU

Über speziell für die Zielgruppe kleine und mittelständische Unternehmen zugeschnittene Warnungen, Tipps und Tricks zum Thema IT-Sicherheit in Unternehmen informiert der BSI-Newsletter. **www.bsi.bund.de**
KMU Newsletter

Den Ernstfall proben

Entscheidend sei, dass Unternehmen den Ernstfall üben. Das Risiko eines erfolgreichen Angriffs sinke, wenn die von den Herstellern bereitgestellten Sicherheitsupdates schnellstmöglich eingespielt werden. Unerlässlich sei zudem ein genauer Überblick über die eigene meist schnell gewachsene IT-Systemlandschaft. Insbesondere gilt es, Systeme und Daten zu identifizieren, die besonders schützenswert sind. Kreutzer warnt: „Wenn etwa Produktionssysteme angegriffen werden, kann eine Cyberattacke bis zur Insolvenz führen." Um Unternehmen auf den Ernstfall vorzubereiten, bietet Athene Systemadministratoren maßgeschneiderte Trainings auf der Fraunhofer Cyber Range an. „Wir zeigen dort ganz praktisch in einem virtuellen Unternehmensnetz-

CHECKLISTE

Mehr IT-Sicherheit im Homeoffice von Mitarbeitern erhöht gleichzeitig das Sicherheitsniveau des gesamten Unternehmens.

- Der Arbeitgeber sollte seinen Mitarbeitern die notwendige IT-Ausstattung für zu Hause zur Verfügung stellen.
- Benutzen Sie sichere Passwörter und schützen Sie Ihre Technik mit regelmäßigen Updates.
- Übertragen Sie erarbeitete Daten regelmäßig auf das zentrale Firmensystem.
- Schützen Sie Ihren WLAN-Router vor unerlaubtem Zugriff.
- Legen Sie sich eine IT-Notfallkarte griffbereit hin, sodass Sie im Fall des Falles schnell reagieren können.
- Stellen Sie sicher, dass nur Sie Zugriff auf die Unternehmens-IT haben.

Quelle: Bundesamt für Sicherheit in der Informationstechnik (BSI)

werk mit Rechnern, Servern und Datenverkehr, wie man IT-Sicherheitsvorfälle erkennt, abwehrt und welche Maßnahmen man einleiten muss", erklärt Dexheimer, der die Cyber-Range-Gruppe leitet.

Prinzip „Zero Trust"

Selbst spezialisierte Unternehmen sind betroffen, wie das Beispiel des Darmstädter IT-Dienstleisters Count and Care zeigt. Im Sommer 2022 waren nach einem Einbruch in dessen IT-Systeme eine Vielzahl von Anwendungen des Mutterkonzerns Entega lahmgelegt, die Hacker kaperten Kundendaten des Energieversorgers und boten diese im Darknet zum Kauf an. Damit sich IT-Angriffe nicht wie Flächenbrände ausbreiten, empfehlen die Forscher den Unternehmen das Prinzip „Zero Trust". Vertraue keinem System, auch nicht deinen eigenen, so das Paradigma. Von jedem Rechner könnte ein Angriff ausgehen, da er gehackt sein könnte. Deshalb müssten die Zugriffsrechte der Rechner, Netze und die der Nutzer aufs Minimum reduziert und besser als bisher überprüft werden. Cloudexperte Krauss weist auf eine weitere Gefahr hin: Es werden nicht nur die Server verschlüsselt und personenbezogene Daten im Darknet veröffentlicht, sondern auch noch alle Daten auf den Storagesystemen automatisch gelöscht, ohne eine Möglichkeit der Wiederherstellung. Denn das Backup wurde ebenfalls verschlüsselt. „Deshalb muss auch das Backup ausreichend geschützt und aktualisiert werden."

Meldung beim BSI

Ist der Ernstfall eingetreten, können angegriffene Unternehmen über ein Formular auf der Website des BSI einen Vorfall melden. Das Lagezentrum leitet dann umgehend Tipps für Sofortmaßnahmen weiter. Das BSI geht nach Recherchen im Darknet aber auch aktiv auf angegriffene Unternehmen zu, oftmals, bevor diese überhaupt den Angriff wahrgenommen haben. „In diesem ver-

DREI FRAGEN AN

Alexander Gurris, Senior Cyber Security Analyst, Hessen CyberCompetenceCenter, über die Sensibilisierung von Mitarbeitern für das Thema IT-Sicherheit

Herr Gurris, knapp 50 Prozent der Cybersicherheits-Vorfälle in Unternehmen sind auf den Faktor Mensch zurückzuführen. Warum schauen sich Firmen diese Schwachstelle nicht genauer an?
Vielen Firmenleitungen ist nicht bewusst, welchen Zugewinn an Sicherheit sie mit regelmäßigen Schulungen zu Angriffsmethoden, kompetenten Ansprechpartnern und festgelegten Notfallabläufen erreichen können.

Was sind die häufigsten Einfallstore für Hacker?
Der bevorzugte Angriffsweg ist die E-Mail. Angreifer versuchen so an vertrauliche Informationen zu gelangen oder verleiten die Empfänger, schadhafte Anhänge zu öffnen. In der deutschen Industrie ist es nach wie vor üblich, Rechnungen im Excel- oder Wordformat zu versenden.

Wie lassen sich Mitarbeiter für das Thema Cybersicherheit besser sensibilisieren?
Die besten Schulungsmethoden führen die Mitarbeitenden spielerisch in das Thema ein. Ständige Ermahnungen per E-Mail führen zur Ablehnung der Thematik.

Die Fragen stellte Petra Menke, IHK Frankfurt.

Foto: Amin Akhter

Dr. Alexander Köppen, Partner, Bereich Cyber Security and Privacy, Pwc Deutschland: „Die wenigsten Unternehmen haben eine Antwort darauf, welchen finanziellen Schaden Cyberrisiken anrichten können."

schlüsselten Teil des Internets veröffentlichen die Ransomware-Gruppen, wen sie angegriffen haben und manchmal sogar schon einen Teil der abgeflossenen Daten. Ziel der Angreifer ist es dabei, den Druck auf die Angegriffenen zu erhöhen", so Bach.

Netzsicherheit erhöhen

Die Zunahme von Cyberattacken ruft immer stärker den Gesetzgeber auf den Plan. Den rechtlichen Rahmen setzt das seit Juli 2015 gültige Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz/IT-SiG). Mit verbindlichen Mindestanforderungen an die IT-Si-

Hessen CyberCompetenceCenter

Um kleine und mittelständische Unternehmen, Einrichtungen der Landes- und Kommunalverwaltung sowie Organisationen oder Einrichtungen mit wichtiger Bedeutung für das staatliche Gemeinwesen (Kritis) in puncto Cybersicherheit zu unterstützen, hat das hessische Innenministerium das Hessen CyberCompetenceCenter (Hessen3C) eingerichtet. Dessen Aufgabe ist es, die Sicherheit in der Informationstechnik des Landes zu erhöhen, cyberspezifische Gefahren abzuwehren sowie die Effizienz der Bekämpfung der Cyberkriminalität zu steigern. Hessen3C arbeitet hierzu eng mit der hessischen Polizei, dem Landesamt für Verfassungsschutz und dem Landeskriminalamt zusammen.

Allianz für Cybersicherheit

Für einen erfolgreichen Umgang mit Cyberrisiken sind für Unternehmen aller Größen und Branchen aktuelle Informationen, Wissens- und Erfahrungsaustausch sowie der stetige Ausbau von Sicherheitskompetenzen unerlässlich. Im Rahmen einer kostenlosen Mitgliedschaft in der Allianz für Cybersicherheit tauschen sich bereits über 6700 Unternehmen aus und arbeiten gemeinsam daran, wie IT-Sicherheitsmaßnahmen angemessen umgesetzt werden können. **www.allianz-fuer-cybersicherheit.de**

Foto: IT-Kanzlei dr-lapp.de

Dr. Thomas Lapp, Rechtsanwalt und Fachanwalt für Informationstechnologierecht: „Wenn Mandanten bei Lösegeldforderungen nach einem Cyberangriff zahlen, ist das einzig Sichere, dass das Geld weg ist."

cherheit verbessert es vor allem den Schutz der Kritischen Infrastrukturen (Kritis) und erhöht die Netzsicherheit in den Bereichen, deren Ausfall oder Beeinträchtigung dramatische Folgen für Wirtschaft, Staat und Gesellschaft in Deutschland hätten. Außerdem besteht eine Verpflichtung von Kritis-Betreibern zur Meldung von erheblichen IT-Sicherheitsvorfällen an das BSI. Um den Schutz den aktuellen Gegebenheiten anzupassen, wurde im April 2021 das IT-Sicherheitsgesetz 2.0 verabschiedet. Demnach müssen alle Kritis-Betreiber spätestens bis zum 1. Mai 2023 erweiterte Sicherheitsmaßnahmen für ihre IT umsetzen.

Existenzbedrohende Schäden

„Verstoßen Unternehmen gegen das Gesetz, droht ihnen nicht nur ein finanzieller Schaden infolge eines Produktionsausfalls, sondern es können auch Schadenersatzforderungen von Kunden kommen", sagt Dr. Thomas Lapp, Rechtsanwalt und zertifizierter Mediator, Fachanwalt für Informationstechnologierecht, Frankfurt. Selbst bei einer kleinen mittelständischen GmbH, die nicht unter das IT-SiG fällt, sei die Unternehmensleitung zur ordnungsgemäßen Unternehmensführung verpflichtet. Dazu zählen auch angemessene Maßnahmen zum Schutz gegen Cyberbedrohungen. „Sichert das Unternehmen die IT nicht entsprechend ab, kann dies sogar zur persönlichen Haftung der Geschäftsführer führen", so Lapp.

„Der GAU wäre, dass das Unternehmen wegen eines längeren Produktionsausfalls Insolvenz anmelden muss. Unternehmen, die eine längere Zeit einen IT-Ausfall erleiden, drohen existenzbedrohende Schäden." Bei Lösegeldforderungen mahnt der Anwalt zur unbeding-

Lagebericht 2022

Mit seinem Bericht zur Lage der IT-Sicherheit in Deutschland legt das Bundesamt für Sicherheit in der Informationstechnik (BSI) als die Cyber-Sicherheitsbehörde des Bundes jährlich einen umfassenden Überblick über die Bedrohungen im Cyberraum vor. In 2022 bewertet der Bericht auch die IT-Sicherheitslage im Kontext des russischen Angriffskrieges auf die Ukraine. **www.bsi.bund.de** Bericht IT-Sicherheit

ten Vorsicht. „Wenn Mandanten zahlen, ist das einzig Sichere, dass das Geld weg ist. Es ist nämlich keinesfalls ausgemacht, dass der Geschädigte im Anschluss wieder Zugriff auf seine Daten beziehungsweise alle Daten bekommt." Die Erpresser könnten zudem nach wie vor die gestohlenen Daten Dritten verkaufen. Und last, but not least, unterstütze man die organisierte Cyberkriminalität.

Cyberpolice: Kosten und Nutzen

Um sich zu schützen, schließen viele Unternehmen eine Cyberversicherung ab oder denken zumindest darüber nach. Aus Sicht von Krauss hat bereits der Assessment-Prozess den Vorteil, dass ein Unternehmen Risiken erkennen kann, derer es sich zuvor gar nicht bewusst war. Anwalt Lapp ergänzt: „Eine Cyberpolice hat den entscheidenden Vorteil, dass der Geschädigte einen gewissen finanziellen Ausgleich, Erstattung von Kosten sowie Unterstützung bekommen kann: Denn egal, wie sich ein Unternehmen geschützt hat, angreifbar ist man immer." Versicherungsnehmer müssten aber genau schauen, welcher Schaden wie abgedeckt ist und welche Ausschlüsse es gibt. Gleichzeitig gelte es, Kosten und Nutzen abzuwägen. Denn die massiv gewachsene Zahl an Cyberangriffen auf Unternehmen führt zu immer aufwendigeren Verhandlungen bei der Absicherung von Risiken. Der Trend geht zu deutlich höheren Prämien bei geringerem Schutz, gestiegenen Selbstbehalten und einer zunehmenden Zahl von Ausnahmen in den Verträgen.

Die neue Normalität

Für die Wirtschaft bleibt Cybersicherheit auch künftig ein Topthema. Die vom Digitalverband Bitkom in 2022 befragten Unternehmen erwarteten in den kommenden zwölf Monaten eine weitere Zunahme von Cyberangriffen. 42 Prozent der Unternehmen rechneten mit einem starken Anstieg, 36 Prozent mit einem eher starken. Gut gerüstet sind die potenziellen Opfer nicht. „Selbst bei gut aufgestellten Unternehmen gibt es noch viele Lücken bei den Mobiltechniken, also Smartphones, die dienstliche Daten, etwa aus der Cloud, abrufen können", stellt Schmidt fest. Und Köppen von PwC ergänzt: „Für den Mittelstand wird das Thema OT-Security (operative Technologie) der Maschinen und Anlagen im Unternehmen immer wichtiger, da IT und OT zunehmend konvergieren. Risiken bestehen zum Beispiel bei der Fernwartung oder den Netzübergängen zwischen IT und Produktionsbereichen." Auch hier müssten die Zuständigkeiten klar definiert und Abwehrfähigkeiten aufgebaut werden. Das sei eine der größten Herausforderungen.

Für Cisco-Manager Krauss steht deshalb fest: „Keine Geschäftsleitung kommt heute darum herum, sich mit Cybersicherheit zu beschäftigen – und das jeden Tag von Neuem, denn die neue Normalität ist das konstante Risiko einer Cyberbedrohung, genauso wie jede andere kritische Unternehmensanforderung." Anwalt Lapp beschreibt die Herausforderung mit dem Balanceakt auf einem großen Gymnastikball, der ständig in Bewegung ist. „Nur wer sich mitbewegt, stürzt nicht ab und schützt so sein Unternehmen bestmöglich vor Cyberattacken."

DIE AUTORIN

Eli Hamacher
Freie Journalistin, Berlin
eh@elihamacher.de