D 7465

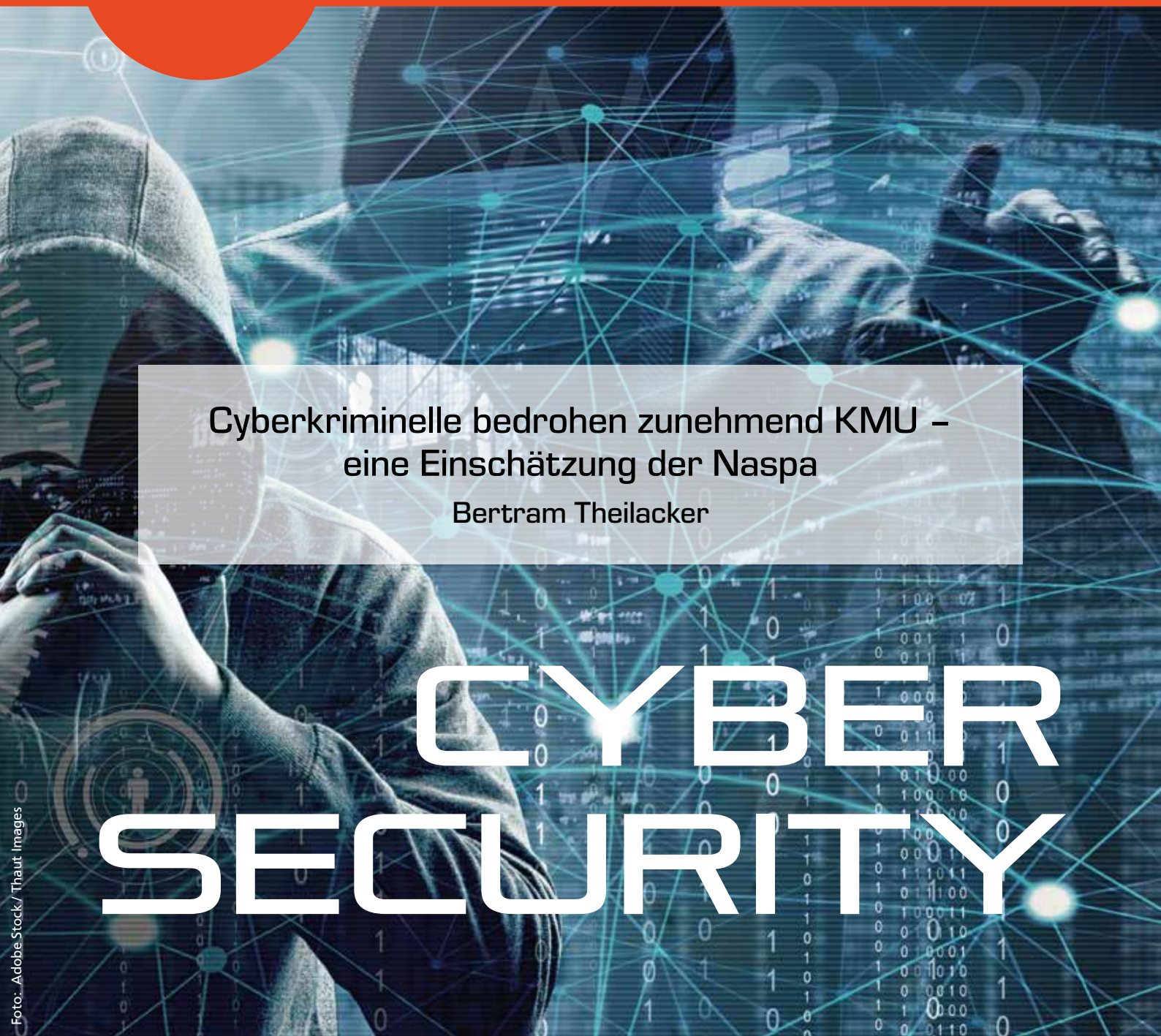
Zeitschrift für das gesamte
REDITWESEN

76. Jahrgang · 1. März 2023

5-2023

Digitaler Sonderdruck

Pflichtblatt der Frankfurter Wertpapierbörse
Fritz Knapp Verlag · ISSN 0341-4019



Cyberkriminelle bedrohen zunehmend KMU – eine Einschätzung der Naspa

Bertram Theilacker

CYBER SECURITY

Foto: Adobe Stock/ Thaut Images

Bertram Theilacker

Cyberkriminelle bedrohen zunehmend **KMU** – eine Einschätzung der Naspa

Sorgen vor einem Cyberangriff hatte sich Patrick R., Geschäftsführer eines mittelständischen Unternehmens für Pumpen und Anlagenbau, nicht gemacht. Er wähnte die Daten seines Betriebs „so sicher wie in Abrahams Schoß". Bis zu jenem Wochenende im Sommer 2021, als der Firmenchef in den Betrieb fuhr, um dort nach dem Rechten zu sehen. Kaum war er in den Büroräumen, wurde ihm unversehens klar, dass irgendetwas nicht stimmen konnte. Die Drucker hatten stapelweise Papier ausgespuckt. Zunächst dachte Patrick R. noch an einen etwas missratenen Scherz seiner Mitarbeiter, doch schnell begriff er, dass der Vorfall alles andere als lustig war. Sein Unternehmen war Zielscheibe eines Cyberangriffs geworden. Alle relevanten Daten waren verschwunden. Die Forensiker des Landeskriminalamtes konnten den Angriff zunächst noch nachvollziehen: Exakt um 23.15 Uhr war die Firewall gehackt worden. Die Spur der Angreifer ließ sich bis Belarus zurückverfolgen, doch dann war Schluss.

„Rabatt" von den Erpressern

Derweil verhandelte Patrick R. mit den Erpressern im Darknet. Die verlangten 50 000 Euro in Bitcoin, um dem Unternehmen wieder Zugang zu den wichtigen Daten zu verschaffen. Und dann – Höhepunkt der Dreistigkeit – räumten die Cyberkrieger dem Unternehmen bei umgehender Zahlung noch 10 Prozent Rabatt ein. Der Mittelständler zahlte und schaffte sofort neue Hardware an. Die Nutzung von Public Cloud, Freeware und Datensticks ist seither verboten. Außerdem macht das Unternehmen nun viel häufiger Backups als früher.

Dieses Beispiel ist kein Einzelfall. Immer stärker geraten kleine und mittelständische Unternehmen in das Visier von Cyberkriminellen. Und mitunter schlagen die Hacker sogar mehrfach zu, wie der Fall eines Frankfurter Dienstleistungsunternehmens belegt. Fast ein Jahr nach der ersten Attacke kam es im Februar 2023 erneut zu einem Cyberangriff. Da das Unternehmen nach dem ersten Vorfall aber erheblich in die IT-Sicherheit investiert hatte, waren die Folgen dieses Mal nach Angaben des Unternehmens weniger gravierend.

Opfer der Cyberkriminellen waren bislang vorrangig Großkonzerne. Im Februar 2023 berichtete Continental, zum Ziel von Cyberattacken geworden zu sein. „Die Untersuchung des Vorfalls hat in der Zwischenzeit ergeben, dass die Angreifer trotz etablierter Sicherheitsvorkehrungen auch einen Teilbestand von Daten aus betroffenen IT-Systemen entwenden konnten", heißt es in einer Pressemitteilung von Continental vom 10. Februar 2023.

Insgesamt 223 Milliarden Euro Gesamtschaden entstehen allein der deutschen Wirtschaft jährlich durch kriminelle Cyberaktivitäten, so das Bundeskriminalamt. Um die Größenordnung begreiflich zu machen: Das entspricht in etwa der Marktkapitalisierung sämtlicher Automobilhersteller im DAX. Die Experten von McKinsey sagen für 2025 einen weltweiten Schaden durch Cyberangriffe in Billionenhöhe voraus. Kein Wunder also, dass Cybersecurity mittlerweile als globaler Wachstumsmarkt gilt.

Mittelständische Unternehmen im Fokus

Je größer die Unternehmen, desto interessanter sind sie für die Hacker. Besonders die digital weltweit vernetzten DAX-Konzerne. Denn dort können eben auch hohe Lösegeldforderungen durchgesetzt werden. Mittlerweile werden auch mehr und mehr kleine und mittelständische Unternehmen zum Ziel der sogenannten Ransomware („Erpressungssoftware").

Mithilfe dieser Software erhalten die Cyberkriminellen Zugriff auf Daten des Unternehmens, deren Nutzung oder auf das gesamte Computersystem und können diese verschlüsseln. Die Entschlüsse-

Die unterschiedlichen cyberkriminellen Gruppierungen

1. Unabhängige Cyberkriminelle: Sie sind in erster Linie finanziell motiviert, möchten also von ihren Opfern Lösegeld erpressen; hinzu kommen sogenannte Hacktivisten, wie etwa Anonymous.

2. State-Sponsored: Lose Kooperation mit Staaten sowie Akzeptanz durch staatliche Strukturen.

3. Staatliche Akteure: Politische Agenda und ideologische Ziele.

Quelle: Bundeskriminalamt, Bundeslagebild Cybercrime 2021, S. 31

lung der Daten oder deren Freigabe erfolgt erst gegen Zahlung eines Lösegeldes, in der Regel in Form von Bitcoin, wie im eingangs angeführten Beispiel.

Während Großunternehmen in den vergangenen Jahren IT-mäßig aufgerüstet haben und sich mehr und mehr gegen Cyberattacken schützen, nehmen die Cyberkriminellen zunehmend kleine und mittelständische Unternehmen in den Fokus ihrer Aktivitäten. Da die Cyberattacken bislang vor allem auf Großunternehmen erfolgten – also dort „wo es etwas zu holen gibt" – herrschte lange Zeit bei den kleinen und mittelständischen Unternehmen eine gewisse Arglosigkeit vor. Allerdings seien auch diese Betriebe zunehmend gefährdet.

Das Thema Cybersicherheit habe noch immer nicht genügend Aufmerksamkeit, warnte jüngst Karl Josef Lutz, seines Zeichens Präsident der Industrie- und Handelskammer (IHK) für München und Oberbayern. „Im schlimmsten Fall steht die Existenz auf dem Spiel. Nur eine entschlossene Prävention kann das immense Potenzial für Schäden durch Cyberangriffe verringern", sagte Lutz unlängst in einem Interview mit dem Bayrischen Rundfunk. Laut einer IHK-Umfrage haben nur rund 42 Prozent der befragten bayerischen Unternehmen entsprechende IT-Notfallpläne. Lediglich 60 Prozent der Betriebe führen Risikoanalysen durch und schulen ihre Mitarbeiter in Sachen IT-Sicherheit. Es ist wohl davon auszugehen, dass sich die Situation in anderen Bundesländern, auch im Geschäftsgebiet der Naspa, nicht signifikant anders darstellt.

225 Fälle allein in Hessen

Bei Cybercrime handle es sich um einen sehr dynamischen Kriminalitätsbereich mit unzähligen Tatmöglichkeiten, berichtet das Hessische Innenministerium. Die Täter beziehungsweise Tätergruppierungen seien aufgrund der immer stärker voranschreitenden Digitalisierung und der Vernetzung nicht an Ländergrenzen gebunden und agierten dementsprechend weltweit.

Im vergangenen Jahr wurden allein der Zentralen Ansprechstelle Cyberkriminalität Hessen (ZAC) 225 Fälle bekannt, in denen Unternehmen sowie öffentliche und nichtöffentliche Stellen in diesem Bundesland Opfer von Cyberangriffen wurden und aus denen Strafanzeigen resultierten. Tatsächlich dürfte die Zahl der Fälle noch höher liegen, weil Experten von einer hohen Dunkelziffer ausgehen. Das heißt, viele Cyberattacken kommen erst gar nicht zur Anzeige. Die ZAC sind in den jeweiligen Landeskriminalämtern angesiedelt.

Im Fall eines Cyberangriffs sind die ZAC in den Bundesländern die ersten Ansprechpartner – auch und gerade für kleine und mittelständische Unternehmen. Die dortigen Mitarbeiterinnen und Mitarbeiter fertigen für die Ereignisfälle Strafanzeigen an und leiten Sofort- und Erstmaßnahmen ein. Die weiterführende Bearbeitung obliegt grundsätzlich den sachlich und örtlich zuständigen Fachdienststellen in den Polizeipräsidien, wobei die Mitarbeiterinnen und Mitarbeiter der ZAC im Bedarfsfall weitere technische Unterstützung und Maßnahmen (zum Beispiel Austausch auf deutscher und europäischer Ebene) koordinieren.

Strategien der Cyberkriminellen

Bei der Suche nach potenziellen Opfern gehen die Cyberkriminellen im Wesentlichen nach zwei Strategien vor. Zum einen suchen sie gezielt nach Unternehmen, die Schwachstellen in ihrer IT-Infrastruktur aufweisen (Motto: „Möglichkeit schafft Täter"). Von dieser Strategie betroffen sind vor allem kleine und mittelständische Unternehmen. Das heißt, in solchen Fällen kann jedes Unternehmen zum Opfer von Cyberkriminellen werden, das nicht ausreichend in eine sichere und nachhaltige IT-Infrastruktur investiert oder eine gewisse Arglosigkeit im Umgang mit diesem Thema an den Tag legt. Von dieser Strategie ist das „Big Game Hunting" zu unterscheiden. Hierbei handelt es sich um einen gezielten Angriff auf umsatzstarke Großkonzerne. Um die Höhe der Lösegeldforderungen zu ermitteln, analysieren die Angreifer beispielsweise die dank des Publizitätsgesetzes verfügbaren Quartals- und Jahresberichte ihrer Opfer.

Trotz aller Bemühungen der Behörden stiegen die Fallzahlen seit 2019 nach einer Statistik des Bundeskriminalamtes weiter an. Parallel dazu fiel die Aufklärungsrate auf unter 30 Prozent. Durch die Verzahnung von (digitalen) internationalen Lieferketten erhöhte sich die Anzahl potenzieller Eintrittsfaktoren für Täter und Schadsoftware.

Bertram Theilacker

Mitglied des Vorstands, Nassauische Sparkasse, Wiesbaden

Cyberkriminelle nahmen noch vor einiger Zeit in erster Linie Großunternehmen ins Visier. Davon kann heute keine Rede mehr sein. Immer häufiger werden auch kleine und mittelständische Unternehmen – also die klassische Klientel der Sparkassen – zu Opfern von Ransomware-Erpressern oder anderen Cyberkriminellen. Dazu bringt der Autor im vorliegenden Beitrag ein reales Beispiel, bei dem ein mittelständisches Unternehmen erpresst wurde. Das Problem: Zwar bieten größere Konzerne höhere Lösegeldmöglichkeiten, doch hätten diese Konzerne in den vergangenen Jahren ihre IT aufgerüstet. Aber auch wenn die kleinen und mittleren Unternehmen aufrüsten, bleibe ein Restrisiko, das man jedoch versichern könne. Beim Thema Cybersecurity sieht Bertram Theilacker eine kongruente Interessenlage zwischen den Sparkassen und den Unternehmen, denn auch für die Sparkassen könnten die Folgen von Cyberangriffen ein Problem werden, wenn dadurch die Kreditausfallgefahr steigt. (Red.)

Bleibt am Ende die essenzielle Frage, was kleine und mitttelständische Unternehmen tun können, um sich vor den Angriffen von Cyberkriminellen zu schützen. Am Anfang steht wie immer die Sensibilisierung der Unternehmen hinsichtlich der beschriebenen Risiken. Dies gilt insbesondere für kleine Unternehmen, die sich vorrangig auf ihren Geschäftszweck konzentrieren und wenig Ressourcen für das Risikomanagement bereitstellen können.

Die gewerblichen Kunden der Naspa werden durch praxisnahe Veranstaltungen und regelmäßig im persönlichen Dialog auf die Risiken und Präventionsmaßnahmen angesprochen. Daneben sind auf der Homepage des Instituts und unter sparkasse.de gut strukturierte Informationen zu finden. Den Kunden mit Sitz in Rheinland-Pfalz und Hessen wird die Zentrale Ansprechstelle Cybercrime (ZAC) beim LKA mit Sitz in Mainz beziehungsweise das HessenCyberCompetence-Center (Hessen3C) empfohlen.

Das Hessen3C ist in Sachen Prävention für mittelständische Unternehmen der zentrale Ansprechpartner für IT-Sicherheitsvorfälle. Es arbeitet eng mit der hessischen Polizei, dem Landesamt für Verfassungsschutz Hessen und dem Hessischen Landeskriminalamt zusammen. Es wurde 2019 im Hessischen Ministerium des Inneren und für Sport als Referat der Abteilung VII – Cyber- und IT-Sicherheit, Verwaltungssicherheit – eingerichtet. Aufgabe des Hessen3C ist es, die Sicherheit in der Informationstechnologie des Landes zu erhöhen, cyberspezifische Gefahren abzuwehren und die Effizienz der Bekämpfung der Cyberkriminalität zu steigern. Nach Angaben des Hessischen Innenministeriums können auch kleine und mittelständische Unternehmen die kostenlosen Leistungen von Hessen3C in Anspruch nehmen.

Passgenaue Lösungen

Trotz aller Präventionsmaßnahmen bleibt ein Restrisiko für die kleinen und mittelständischen Unternehmen. Und auch dieses Restrisiko kann man absichern. Denn die Schäden, die durch Cyberkriminalität entstehen, sind teilweise exorbitant hoch. Sie beschränken sich nicht allein auf die Höhe der möglichen Lösegelderpressung, vielmehr kommt es gerade bei mittelständischen Betrieben in der Regel zu langwierigen Betriebsunterbrechungen. Sprich: Es kann nichts mehr produziert und nichts mehr verkauft werden. Auch die Zahl der sogenannten Supply-Chain-Angriffe ist nach Erkenntnissen des Bundeskriminalamtes in den vergangenen Jahren deutlich gestiegen.

Die dadurch ausgelösten Lieferkettenunterbrechungen haben teilweise internationale Konsequenzen – auch für mittelständische Unternehmen, die stark globalisiert sind. In der Folge fehlen Einnahmen, Rechnungen können vorübergehend nicht beglichen werden. Manche kleine und mittelständische Betriebe berichten, dass sie sogar die Löhne und Gehälter an ihre Mitarbeiter erst mit Verspätung auszahlen konnten.

Es erscheint also empfehlenswert, sich für den Fall der Fälle entsprechend abzusichern. Verschiedene Versicherungsgesellschaften bieten maßgeschneiderte Lösungen an. Zum Beispiel die SV SparkassenVersicherung. Interessant für kleine und mittelständische Unternehmen ist vor allem der SV CyberSchutz. Für größere Schäden bietet die SV zusammen mit ihrem Kooperationspartner AIG das Produkt CybeEdge. Dieser weitergehende Versicherungsschutz eignet sich für Betriebe bis 150 Millionen Euro Umsatz.

Interessengleichheit Kunde/Sparkasse

Zwischen gewerblichen Kunden und der Naspa besteht erkennbar eine Interessengleichheit. Die gezielte Reduzierung der Risiken aus Cyberkriminalität ist sowohl im Sinne des Unternehmens als auch der Sparkasse. Die Vorteile für die Unternehmen liegen auf der Hand. Aber auch für die Sparkasse können die Folgen von Cyberkriminalität ein Problem werden, denn dadurch steigt gegebenenfalls die Ausfallwahrscheinlichkeit eines Kreditengagements unmittelbar und signifikant. Folglich ist für die Naspa unter anderem die Datensicherheit bei gewerblichen Kunden im Rahmen der Kreditwürdigkeitsprüfung ein wichtiges Kriterium.

Welche Arten von Cyberangriffen auf Unternehmen gibt es?

1. Online-Erpressung durch die sogenannte Ransomware: Die Unternehmensdaten werden verschlüsselt und erst wieder freigegeben, wenn die Firma ein Lösegeld zahlt (Lösegelderpressung). Das Schadenspotenzial von Ransomware nimmt seit Jahren rasant zu. Laut der Studie „Wirtschaftsschutz 2021" des Bitkom e.V. ist der jährliche Schaden von Ransomware in Deutschland 2021 auf rund 24,3 Milliarden Euro gestiegen. Im Jahr 2019 betrug diese Zahl noch 5,3 Milliarden Euro. Laut Chainalysis haben Ransomware-Gruppierungen im Jahr 2021 rund 602 Millionen US-Dollar in Form von Kryptowährungen erpressen können. Nach Erkenntnissen des BKA ist Deutschland im internationalen Vergleich überdurchschnittlich häufig von Ransom-Angriffen betroffen und git als eines der häufigsten Ziele von Ransomware-Akteure.

2. Online-Erpressung durch DDoS-Angriffe (DDoS = Destributed-Denial-of-Service): Die Webseite eines Unternehmens wird durch übermäßige Anfrage lahmgelegt.

3. Man-in-the-Middle-Angriffe: Täter fangen E-Mails ab und verändern diese, zum Beispiel Rechnungen.

4. Datendiebstahl: Täter stehlen Kunden- und Bankdaten sowie Adressen und verkaufen diese.

5. CEO-Fraud: Täter erwirken unter Vorspiegelung falscher Identität hohe Überweisungen.

Cyberschutz für Unternehmen

Absicherung, Schaden- und Krisenmanagement aus einer Hand. Schützen Sie Ihr Unternehmen wirksam gegen Internet-kriminalität.

naspa.de/cyberversicherung

Naspa
Nassauische Sparkasse