PRODUKTION IM VISIER

Wie Mittelständler sich vor Cyberangriffen schützen

Die Gefahr Opfer eines IT-Angriffs zu werden, ist groß. Oft genügt ein Einfallstor und die Sicherheit ist gefährdet. Wie sich Unternehmen schützen können und wie wichtig Security auch bei der Entwicklung von Software ist, erklärt Prof. Dr. Eric Bodden, Direktor des Fraunhofer IEM in Paderborn, Abteilung Softwaretechnik, und Vorstand des Heinz Nixdorf Instituts der Universität Paderborn.

Sie beschäftigen sich seit vielen Jahren mit der IT-Sicherheitsforschung. Wo sehen Sie den größten Bedarf für innovative IT-Sicherheitslösungen?
Dr. Eric Bodden: Es muss uns besser gelingen, Angreifern den Einstieg in unsere Systeme zu verhindern. Ein großes Problem ist dabei Phishing, bei dem mittels täuschend echter E-Mails Angestellte dazu verleitet werden, ihre Kennwörter auf Webseiten einzugeben, die der Angreifer kontrolliert. Da nun auch Angreifer ChatGPT etc. nutzen können, wird Phishing immer schwerer zu erkennen. Was mich hier positiv stimmt, ist, dass wir mittlerweile gut nutzbare und sichere Verfahren zur passwortlosen Authentisierung haben. Apple, Google und Microsoft haben vor einigen Wochen zeitgleich angefangen, sogenannte „Passkeys" anzubieten. Das sind automatisch generierte Schlüssel, die Sie sicher und mit einem Fingerabdruck geschützt auf Ihrem Handy oder in Ihrem Webbrowser abspeichern können. Ein Passwort braucht es dann nicht mehr, Sie loggen sich nur über einen Fingerabdruck ein. Damit laufen dann Phishing-Angriffe ins Leere – ein großer Sicherheitsgewinn!

„Security by Design" ist ein Konzept, das sicherstellt, dass Sicherheitsanforderungen bereits zu Beginn des Entwicklungsprozesses systematisch ermittelt und berücksichtigt werden, um spätere Aufwände zur Behebung von Sicherheitslücken zu verhindern oder zu minimieren. Wie beurteilen Sie den aktuellen Entwicklungsstand?
Dr. Eric Bodden: Die große Achillesferse der IT-Sicherheit ist seit Jahren die Software. Die allermeisten Angriffe nutzen eigentlich recht banale Schwachstellen in Anwendungssoftware aus. Hier müssen Unternehmen, die Software produzieren, systematisch umdenken und diese Software von Grund auf sicher entwickeln – eben mittels Security by Design. Der Stand der Forschung ist schon recht weit. Wenn Unternehmen ihre Softwareentwicklung nach dem aktuellen Stand der Forschung gestalten würden, wäre schon viel gewonnen und Softwareschwachstellen wären sehr viel weniger wahrscheinlich. Leider haben bisher Marktzwänge den Unternehmen eher die falschen Anreize gesetzt. Startups und KMU müssen mit einer Software oft die Ersten im Markt sein, um schnell Marktanteile zu gewinnen. Über Security denkt man dann oft erst nach, wenn das Softwareprodukt Erfolge feiert und eine breite Nutzerbasis findet – doch dann ist es für Security by Design schon zu spät. Die EU möchte hier noch in diesem Jahr mit dem sogenannten Cyber Resilience Act nachsteuern. Wenn dieser so umgesetzt wird, wie der aktuelle Entwurf aussieht, dann werden in Zukunft Unternehmen, die in der EU Software auf den Markt bringen, zunehmend strikte Mindeststandards im Hinblick auf die sichere Entwicklung einhalten müssen. Ein guter Zeitpunkt, um Security by Design endlich anzupacken und umzusetzen! Am Fraunhofer IEM beraten wir schon seit vielen Jahren sehr umfassend Unternehmen in diesen Prozessen.

Das Internet of Things bietet immer mehr Kommunikations- und Vernetzungsmöglichkeiten. Dadurch erhöhen sich jedoch auch die potenziellen Risiken. Wie lassen sich Bedrohungen möglichst schon im Vorfeld erkennen, ohne dass es zu größeren Schäden kommt?
Dr. Eric Bodden: Wichtig ist, dass, wenn ein IT-Produkt eingesetzt wird – sei es ein IoT-Gerät oder auch „nur" eine Software – dass dies unter der genauen Betrachtung der möglichen Sicherheitsrisiken geschieht, die damit einhergehen. Das Standardwerkzeug hierzu ist die Bedrohungsanalyse. Hier werden zunächst mögliche Angreiferpersonas definiert: Wer könnte logischerweise angreifen wollen und warum und mit welchen Mitteln? Als Nächstes definiert man dann schützenswerte „Assets" und diskutiert, inwiefern diese aktuell bereits gegen diese Angreifer geschützt wären und wo man ggf. wie nachsteuern müsste. Konkret kann dies dann bedeuten, dass man ein IoT-Gerät nur in einer besonders geschützten Umgebung einsetzt oder seine Software härtet oder es vielleicht auch gar nicht verwendet, sondern durch eine sicherere Variante ersetzt. Die Fähigkeit, eine Bedrohungsanalyse durchzuführen, sollte für eigentlich alle Technologieunternehmen heute zum Handwerkszeug gehören. Und dieses Handwerk kann man schnell erlernen, auch hierzu bieten wir und andere Fortbildungen an.

Prof. Dr. Eric Bodden, Direktor des Fraunhofer IEM, Abteilung Softwaretechnik
Foto: Universität Paderborn

„Ein großes Problem in der sicheren Softwareentwicklung ist das Einbinden von unsicherem Programmcode von Drittanbietern."

CYBER-SICHERHEIT

Zu wenig Risikobewusstsein

Cyberangriffe sind eine tägliche Bedrohung für Unternehmen. Dennoch hinken viele beim Schutz hinterher, weil sie die Risiken unterschätzen.

Die Bedrohungslage ist ernst – diese Aussage ist zunächst einmal wenig überraschend, schließlich hören wir seit Jahren, dass die Angriffe von Cyberkriminellen zunehmen und immer raffinierter werden. Das Besondere der vor einigen Monaten vom Bundesamt für Sicherheit in der Informationstechnik (BSI) und TÜV-Verband veröffentlichten repräsentativen Umfrage zur Cybersicherheit in Unternehmen ist allerdings, dass viele befragten Firmen die Lage unterschätzen und die eigene Resilienz überbewerten. Das BSI warnt vor trügerischer Sicherheit. Schließlich sind laut Studie gut 15 Prozent der Unternehmen im vergangenen Jahr Opfer einer Cyberattacke geworden. Besonders häufig wurden Phishing-Angriffe verzeichnet. Auch Lieferketten seien eine Gefahr. Angegriffen würden insbesondere Ingenieurbüros und IT-Firmen. Häufig stelle sich erst später heraus, dass nicht sie das eigentliche Angriffsziel waren, sondern deren Kunden. Doch inzwischen beschränken sich Lieferketten-Angriffe, sogenannte Supply Chain Attacks, nicht mehr auf klassische Software-Lieferketten.

Auch KI-Systeme stehen im Visier. In der Nutzung erscheinen diese häufig als Black-Box, doch anders als angenommen, bestehen sie nicht aus einem kompakten Software-Block. Verschiedene Komponenten fließen in eine typische KI ein, Systeme sind aus verschiedensten Modulen aufgebaut, dabei wird auch massiv auf Software-Bibliotheken zurückgegriffen. Zudem können generische KI-Systeme je nach Anwendungszweck neu zusammengesetzt und Module ausgetauscht werden, warnen KI-Spezialisten. So fügen Entwickler Komponenten wie Modelle, Plug-ins und Trainingsdaten je nach Bedarf zusammen. Experten raten angesichts der Gefahrenlage dazu, Software-Stücklisten einzuführen, wie es in anderen industriellen Produktionsbereichen üblich ist. Sie sorgen für Transparenz und Nachverfolgbarkeit in der Software-Lieferkette und unterstützen dabei, Schwachstellen zu identifizieren und die Compliance der eingesetzten Software zu belegen.

Besorgniserregend aus Sicht des BSI ist zudem die Tatsache, dass nur etwa die Hälfte der Befragten die zweite EU-Richtlinie zur Netzwerk- und Informationssicherheit (NIS-2) kennt. Mit der Umsetzung der NIS-2-Richtlinie in nationales Recht, die in Deutschland bisher nicht erfolgt ist, wird das BSI für deutlich mehr Unternehmen als zuvor Aufsichtsbehörde. Für die bestehenden Kritischen Infrastrukturen (KRITIS) ändert sich hierdurch voraussichtlich wenig, aber für etwa 29.000 nach der NIS-2-Richtlinie „wesentliche“ und „wichtige“ Einrichtungen ergeben sich erstmals gesetzliche Pflichten.

„Die deutsche Wirtschaft steht im Fadenkreuz staatlicher und krimineller Hacker, die sensible Daten erbeuten, Geld erpressen oder wichtige Versorgungsstrukturen sabotieren wollen. Allerdings scheinen viele Unternehmen die Risiken zu unterschätzen“, so Dr. Michael Fübi, Präsident des TÜV-Verbands.

BSI-Präsidentin Claudia Plattner sieht noch eine Menge Arbeit, die dringend erledigt werden muss: „Was mich besonders besorgt, ist die geringe Bekanntheit der NIS-2-Richtlinie. Umso wichtiger ist ihre zügige Umsetzung in nationales Recht. Verständlicherweise weisen Unternehmen darauf hin, dass regulatorische Vorgaben herausfordernd sind: auch, weil sie zu Bürokratie und damit zu Mehraufwand führen können. Richtig umgesetzt können sie uns aber dabei helfen, die Resilienz unserer Wirtschaft umfassend zu erhöhen.“

IT-Sicherheit als Gesamtkonzept

Alarmierend ist auch der Anstieg von Schadprogrammen. Im August diesen Jahres wurden laut BSI mehr als sieben Millionen neue Schadprogramm-Varianten bekannt. Hinzu kamen rund 0,2 Millionen neue Varianten potenziell unerwünschter Anwendungssoftware PUA (Potentially Unwanted Application or Applications). Schutz gegen Angriffe mit Schadprogrammen bietet neben regelmäßigen Sicherheitsupdates unter anderem Antivirensoftware, die die Schadsoftware entdeckt, an einer erfolgreichen Ausführung hindert und vom System wieder entfernen kann. Das BSI rät jedoch, sich nicht auf klassische AV-Lösungen und Firewalls allein zu verlassen, sondern IT-Sicherheit als Gesamtkonzept unter Einbeziehung der Nutzer umzusetzen.

Gefahr geht zudem auch von Botnetzen aus. Der Unique-IP-Index, der das Aufkommen und die Entwicklung der infizierten Systeme in den vom BSI beobachteten Botnetzen misst, lag im August 2025 sehr hoch. Die Zahl der infizierten Systeme, die täglich in Botnetzen aktiv sind, lag dem BSI zufolge über zehnmal so hoch wie im Jahresdurchschnitt 2019. Als besonders gefährlich gilt das Botnetz „badbox“, eine Android-Schadsoftware, die mit der Firmware des Geräts ausgeliefert wird. Infizierte Geräte verbinden sich unverzüglich mit einem Command-and-Control (C2)-Server und ermöglichen den Angreifern Zweifaktor-Schlüssel abzufangen, weitere Schadsoftware zu installieren sowie Zugriff auf das IT-Netz, in dem sich das infizierte Gerät befindet (Proxy), zu erhalten.

Informationen des BSI zufolge, ist die Schadsoftware badbox bereits beim Kauf auf den jeweiligen Geräten installiert. Das BSI leitet derzeit im Rahmen einer Sinkholing-Maßnahme die Kommunikation betroffener Geräte mit den Kontrollservern der Täter um. „Dies betrifft Provider, die über 100.000 Kundinnen und Kunden haben. Für diese Geräte besteht keine akute Gefahr, solange das BSI die Sinkholing-Maßnahme aufrechterhält. Grundsätzlich besteht aber für alle IT-Produkte mit veralteten Firmware-Versionen das Risiko, dass sie für Schadsoftware anfällig sind“, so ein BSI-Pressesprecher. Das BSI unterrichtet regelmäßig die zuständigen Netzbetreiber und Internet-Provider über die in den beobachteten Botnetzen detektierten infizierten Systeme, damit diese ihrerseits bei den Betreibern dieser Systeme auf eine Bereinigung hinwirken können. Das BSI geht von einer sehr hohen Dunkelziffer betroffener Geräte aus und ruft dazu auf, entsprechende Geräte vom Internet zu trennen oder nicht weiter zu benutzen. I

Bei den Ausgaben für IT-Sicherheit müssen die Unternehmen dringend zulegen.

Bitkom-Präsident. Achim Berg

DATENSCHUTZ

Angriff aus dem digitalen Raum

Ein Cyberangriff kann Unternehmen hart treffen und sie sogar in ihrer Existenz gefährden. Das weiß auch der Mittelstand. Dennoch lassen die bisherigen Investitionen in geeignete Sicherheitsmaßnahmen zu wünschen übrig.

Die Zahlen sind alarmierend: Durch Diebstahl von IT-Ausrüstung und Daten, Spionage und Sabotage entsteht der deutschen Wirtschaft ein jährlicher Schaden von rund 203 Milliarden Euro. In den Jahren 2018/2019 waren es erst 103 Milliarden Euro. Das sind Ergebnisse einer Studie im Auftrag des Digitalverbands Bitkom, für die mehr als 1.000 Unternehmen quer durch alle Branchen repräsentativ befragt wurden. Praktisch jedes Unternehmen in Deutschland wird Opfer: Dabei sind die Angriffe aus Russland und China zuletzt sprunghaft angestiegen. Zugleich gehen die Angreifer immer professioneller vor. Erstmals liegen das organisierte Verbrechen und Banden an der Spitze der Rangliste der Täterkreise. Bei gut der Hälfte der betroffenen Unternehmen kamen Attacken aus diesem Umfeld. „Spätestens mit dem russischen Angriffskrieg gegen die Ukraine und einer hybriden Kriegsführung auch im digitalen Raum ist die Bedrohung durch Cyberattacken für die Wirtschaft in den Fokus von Unternehmen und Politik gerückt. Die Bedrohungslage ist aber auch unabhängig davon hoch“, sagt Bitkom-Präsident Achim Berg. „Die Angreifer werden immer professioneller und sind häufiger im organisierten Verbrechen zu finden, wobei die Abgrenzung zwischen kriminellen Banden und staatlich gesteuerten Gruppen zunehmend schwerfällt. Allerdings zeigen die Ergebnisse auch, dass Unternehmen mit geeigneten Maßnahmen und Vorsorge dafür sorgen können, dass Angriffe abgewehrt werden oder zumindest der Schaden begrenzt wird.“

Für Verfassungsschutz-Vizepräsident Sinan Selen spiegeln sich die Studienergebnisse auch in der Lageeinschätzung der Cyberabwehr des Bundesamts für Verfassungsschutz wider. „Die Grenzen zwischen Cyberspionage und Cybercrime verschwimmen zunehmend. Wir müssen uns nicht nur auf ein ‚Outsourcing‘ von Spionage einstellen, sondern auch darauf, dass Staaten Cybercrime als Deckmantel für eigene Operationen nutzen. Wir stellen eine Vermischung analoger und digitaler Angriffsvektoren fest. Zudem wechseln staatliche Akteure ihr Zielspektrum flexibel, je nach politischer Agenda, von Wirtschaft zu Politik und umgekehrt.“

Angriffe verlagern sich zunehmend in den digitalen Raum

Angriffe auf die Wirtschaft haben sich weiter in den digitalen Raum verlagert. Gut 60 Prozent der befragten Unternehmen berichten vom Diebstahl sensibler Daten, bei 57 Prozent wurde digitale Kommunikation ausgespäht und 55 Prozent sind von der digitalen Sabotage von Systemen oder Betriebsabläufen betroffen. Leicht rückläufig sind dagegen der analoge Diebstahl von physischen Dokumenten, Unterlagen oder Mustern, das Abhören von Besprechungen oder Telefonaten sowie die analoge Sabotage. „Unternehmen in Deutschland haben seit Beginn der Corona-Pandemie die Digitalisierung vorangetrieben. Damit verlagern sich auch die Angriffe zunehmend in den digitalen Raum“, so Berg.

Beim Diebstahl digitaler Daten haben es die Angreifer verstärkt auf Daten Dritter abgesehen, etwa auf die Entwendung von Kommunikationsdaten wie E-Mails. Bei fast jedem Zweiten waren Kundendaten im Visier. Berg: „Die Täter scheinen genau zu wissen, an welcher Stelle sie am härtesten zuschlagen können. Wenn Daten Dritter entwendet werden, droht den Unternehmen zusätzlicher Schaden. Der reicht von Reputationsverlust bis hin zu möglichen Bußgeldern der Aufsichtsbehörden.“ In jedem dritten betroffenen Unternehmen wurden unkritische Business-Informationen oder Cloud-Zugangsdaten gestohlen. Jedes vierte Unternehmen meldet den Verlust kritischer Business-Informationen wie Marktanalysen sowie Daten von Mitarbeiterinnen und Mitarbeitern. In rund jedem fünften betroffenen Unternehmen hatten es die Täter auf geistiges Eigentum wie Patente abgesehen.

Betreiber kritischer Infrastrukturen erleben zudem einen starken Anstieg von Cyber-Attacken. Die Sorgen vor den Folgen dieser Angriffe wachsen: Etwa 45 Prozent der Unternehmen sehen hierdurch ihre geschäftliche Existenz bedroht.

Bei den Cyberangriffen wurden vor allem Attacken auf Passwörter, Phishing und die Infizierung mit Schadsoftware bzw. Malware für die Unternehmen teuer. Dahinter folgen DDoS-Attacken, um IT-Systeme lahmzulegen. Ransomware-Attacken haben in gut zehn Prozent der Unternehmen Schäden verursacht, das ist nach dem Rekordjahr 2021 mit 18 Prozent ein deutlicher Rückgang. „Bei Ransomware gilt: Durch technische Vorkehrungen und Schulung der Beschäftigten lassen sich Angriffe abwehren. Und wer aktuelle Backups zur Verfügung hat und einen Notfallplan aufstellt, der kann den Schaden einer erfolgreichen Attacke zumindest deutlich

reduzieren“, so Berg. „Auf keinen Fall sollte ein Lösegeld gezahlt werden. Häufig erhalten die Opfer ihre Daten selbst dann nicht in einem brauchbaren Zustand zurück – und zugleich werden die Täter zu weiteren Angriffen motiviert, und die können auch dasselbe Unternehmen erneut treffen.“

Einen Anstieg gab es beim sogenannten Social Engineering. Fast jedes zweite Unternehmen berichtet von entsprechenden Versuchen. Dabei wird vor allem und deutlich häufiger als in der Vergangenheit versucht, über das Telefon und über E-Mail an sensible Informationen zu gelangen. Sie können dann für Cyberattacken verwendet werden. Achim Berg: „Eine regelmäßige Schulung von Mitarbeiterinnen und Mitarbeitern zu Sicherheitsfragen, damit sie sich auch bei Social-Engineering-Versuchen richtig verhalten, sollte in jedem Unternehmen selbstverständlich sein.“

Die Unternehmen erwarten in den kommenden Monaten eine weitere Zunahme von Cyberangriffen. Die Betreiber kritischer Infrastruktur stellen sich sogar auf noch heftigere Attacken ein. Die Wirtschaft fürchtet dabei vor allem Ransomware-Angriffe, dahinter folgen Zero-Day-Exploits und Spyware-Attacken. Mögliche Angriffe mit Quantencomputern als künftige Bedrohung bereiten außerdem Sorgen. Aber auch Entwicklungen auf dem Arbeitsmarkt beunruhigen die Unternehmen: 72 Prozent sehen den Mangel an IT-Sicherheitsexperten als Bedrohung, 58 Prozent die zunehmende Fluktuation von Beschäftigten.

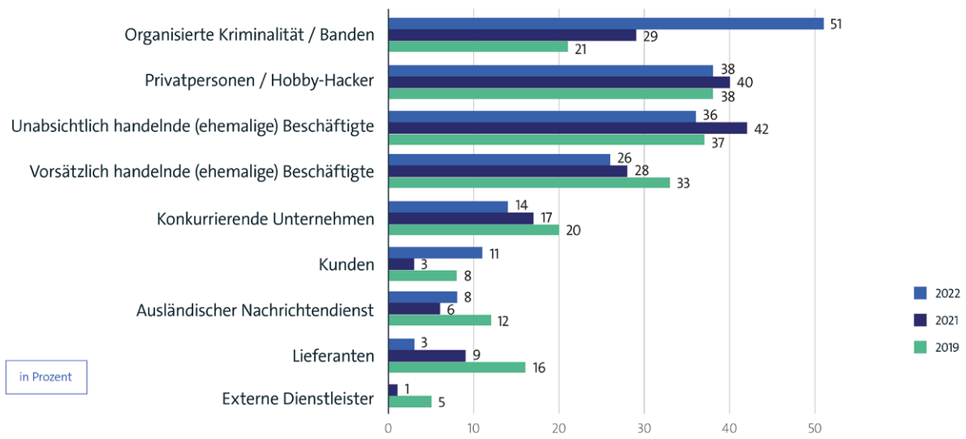
Der Anteil der Ausgaben für IT-Sicherheit am IT-Budget der Unternehmen ist verglichen mit dem Vorjahr leicht gestiegen. Knapp zehn Prozent geben die Unternehmen im Schnitt aus. „Bei den Ausgaben für IT-Sicherheit müssen die Unternehmen dringend zulegen. Die Erkenntnis, welche dramatischen Folgen ein erfolgreicher Angriff haben kann, ist längst da – den notwendigen Schutz davor gibt es aber nicht zum Nulltarif,“ sagt der Bitkom-Präsident. Auch Ausgaben für eine Cyberversicherung gegen Hackerangriffe stehen für viele Unternehmen nicht an vorderster Stelle, obwohl die Furcht vor Cyberkriminalität als eine der größten Gefahren für kleine und mittelständische Unternehmen (KMU) gesehen wird, wie eine aktuelle Studie der Gothaer feststellt. Nur 20 Prozent der KMU haben sich demnach für diese Art der Absicherung entschieden. Das wichtigste Kriterium bei der Auswahl einer Cyberpolice sind Assistance-Leistungen im Schadenfall (53 Prozent), 2019 war dies nur für 45 Prozent der Unternehmen ausschlaggebend. An Relevanz dazugewonnen haben 2023 angebotene Präventionsmaßnahmen (38 Prozent versus 2022: 35 Prozent) sowie die Höhe der Beiträge (48 Prozent, 2022: 45 Prozent). I

Die Grenzen zwischen Cyberspionage und Cybercrime verschwimmen zunehmend

Verfassungsschutz-Vizepräsident Sinan Selen

Attacken auf die Wirtschaft werden professioneller

Von welchem Täterkreis gingen Handlungen in den letzten 12 Monaten aus?



Basis: Alle befragten Unternehmen, die in den letzten 12 Monaten (2019: 2 Jahren) von Diebstahl von Datendiebstahl, Industriespionage oder Sabotage betroffen waren (2022: n=899; 2021: n=935; 2019: n=801) | Mehrfachnennungen möglich | Quelle: Bitkom Research 2022

bitkom

CYBERSICHERHEIT

Wie KI als Katalysator wirkt

Angriffe von Cyberkriminellen auf Unternehmen werden immer komplexer und gefährlicher. Der zunehmende Einsatz von KI schafft zusätzliche Risiken. Warum Betriebe bei der Cyberresilienz umdenken müssen und wie KI bei der Gefahrenabwehr auch nützlich und ein Katalysator sein kann.

Wenn es um Mailangriffe gehe, dann habe man in den letzten Jahren deutlich beobachten können, wie komplex diese geworden seien, sagt Christoff Gosse. „Derzeit identifizieren wir 80 Prozent der eingehenden E-Mails als Phishing oder Spam – und die Angreifer werden immer raffinierter", betonte der IT-Sicherheitsspezialist im Hause dSPACE auf der Veranstaltung „KI und Cyber Security" der Fachhochschule der Wirtschaft (FHDW), ein Format, das vom Bundesforschungsministerium im Rahmen der Forschungsinitiative Arbeitswelt.Plus gefördert wird. Das Paderborner Software- und Elektronikunter-nehmen setze deshalb in der Mail-Security auf Künstliche Intelligenz: Seit 2020 überprüft das KI-gestützte Tool „Darktrace" alle ein- und ausgehenden E-Mails auf ihre Plausibilität in Bezug auf Absender, Empfänger, Häufigkeit und Inhalte. „Mit dieser Lösung hatten wir schon nach kurzer Zeit gute Erfolge. Es bleibt die Frage: Wie lange?", so der IT-Sicherheitsexperte.

Christoff Gosse spricht vielen IT-Sicherheitsverantwortlichen aus der Seele. E-Mails mit schadhaftem Inhalt, die tagtäglich in den Postfächern der Computer landen, sind schon lange eine ernsthafte Bedrohung und gelten als einer der am häufigsten verwendeten Angriffsvektoren für Cyberkriminelle. Schließlich sind E-Mails am Arbeitsplatz allgegenwärtig, die meisten Mitarbeiter verwenden sie, sodass die Wahrscheinlichkeit hoch ist, dass sie ihr Ziel erreichen. Darüber hinaus sind Phishing- und andere E-Mail-basierte Angriffe einfach durchzuführen und können für einen Angreifer erhebliche Gewinne mit sich bringen.

Doch das ist längst nicht die einzige Gefahr. Die Bedrohungen, die von Ransomware ausgehen, werden immer raffinierter, wie der eco – Verband der Internetwirtschaft e. V. betont, und fordert eine konsequente Umsetzung von „Security by Design" und ein deutliches Umdenken bei der Cyberresilienz in Unternehmen. Ransomware-Angriffe führen nicht nur zur Verschlüsselung sensibler Daten, sondern zunehmend auch zum Ausfall von Produktionssystemen oder kritischer Infrastruktur. Datendiebstahl und das gezielte Veröffentlichen vertraulicher Unternehmensdaten sind dabei immer häufiger Bestandteil der Erpressungsstrategie. Kriminelle Akteure setzen auch verstärkt auf künstliche Intelligenz, um Angriffstechniken zu automatisieren und gezielt Schwachstellen auszunutzen. Besonders die Industrie wird immer häufiger zum Ziel – oft mit erheblichen wirtschaftlichen Folgen.

Das Bundeslagebild Cybercrime 2024 des Bundeskriminalamts (BKA) zeigt: Cyberangriffe nehmen weiter zu – mit Ransomware als dominierender Bedrohung. Mehr als 130.000 Straftaten wurden registriert, dazu rund 200.000 Auslandstaten. Die Aufklärungsquote bleibt mit 32 Prozent besorgniserregend niedrig. Parallel warnt das Allianz Risk Barometer 2024 weltweit vor Cybervorfällen als größtem Geschäftsrisiko – besonders durch Erpressungssoftware. Diese Zahlen zeigen: Ohne präventive Maßnahmen und robuste Sicherheitskonzepte reicht der Schutz durch Versicherungen nicht aus. „Ransomware ist kein Randphänomen mehr – sie ist ein strukturelles Risiko für Wirtschaft, Gesellschaft und Staat. Unternehmen müssen nicht nur reaktiv auf Vorfälle reagieren, sondern proaktiv Sicherheitsarchitekturen etablieren. Security by Design ist hier der Schlüssel – und der Cyber Resilience Act macht deutlich, dass dies künftig nicht mehr optional ist", so Prof. Dr. Norbert Pohlmann, eco Vorstand für IT-Sicherheit.

Die Cybersicherheitslandschaft befindet sich seit langem in einem radikalen Wandel. Technologien wie Künstliche Intelligenz (KI) und Quantencomputing eröffnen nicht nur neue Möglichkeiten, sondern schaffen auch neuartige Bedrohungen, wie eco-Sicherheitsexperte Oliver Dehning betont. „Gleichzeitig führen hybride Arbeitsmodelle, der Ausbau von IoT-Ökosystemen und die zunehmende Vernetzung kritischer Infrastrukturen dazu, dass traditionelle Sicherheitsansätze nicht mehr ausreichen. Unternehmen stehen vor der Herausforderung, sowohl mit technologischen Innovationen als auch mit immer ausgefeilteren Angriffsstrategien Schritt zu halten."

Die rasante Entwicklung von KI-Tools habe deren Einsatzschwelle drastisch gesenkt. Heute könnten selbst technisch wenig versierte Angreifer leistungsfähige KI-Systeme einsetzen, um Angriffe zu optimieren, so der Sicherheitsexperte. Gleichzeitig seien Bedrohungen immer komplexer und für den Menschen allein schwer zu erkennen: „KI-basierte Verteidigungssysteme sind notwendig, um diese Herausforderungen zu bewältigen, indem sie verdächtige Aktivitäten in Echtzeit analysieren und bekämpfen. Künstliche Intelligenz bleibt damit sowohl ein mächtiges Werkzeug als auch eine Herausforderung", sagt Dehning.

> **Künstliche Intelligenz und Quantencomputing eröffnen nicht nur neue Möglichkeiten, sondern schaffen auch neuartige Bedrohungen.**

> **Ransomware-Angriffe führen nicht nur zur Verschlüsselung sensibler Daten, sondern zunehmend auch zum Ausfall von Produktionssystemen.**

Zudem haben Digitalisierung und Vernetzung von Unternehmen und Lieferketten in den letzten Jahren zugenommen. Sie bieten viele Vorteile, weil Cloud-basierte Tools, IoT-Integrationen und Remote-Zugriffe die Zusammenarbeit erleichtern, gleichzeitig bergen sie auch neue Risiken. Cyberkriminelle setzen verstärkt auf diese Taktik, da Angriffe auf Zulieferer oft weniger gut abgesichert sind als Angriffe auf große Unternehmen selbst. Hinzu kommt ein wachsender Druck durch regulatorische Anforderungen wie die NIS2-Richtlinie der EU, die explizit stärkere Sicherheitsstandards für Lieferketten fordert.

Auch die Verbreitung von Täuschungstechnologien wird durch Fortschritte in KI und die massive Reichweite sozialer Medien begünstigt. Experten warnen, Unternehmen würden gezielt mit Fake-Informationen manipuliert – sei es durch täuschend echte Mails von „Führungskräften" oder durch gefälschte Audionachrichten, die dringende Überweisungen fordern. „Diese Angriffe stellen nicht nur finanzielle, sondern auch reputationsbezogene Risiken dar. Sicherheitslösungen zur Erkennung und Abwehr solcher Täuschungen sind entscheidend, um Vertrauen in die Kommunikation zu gewährleisten", so Oliver Dehning. Unternehmen müssten proaktiv Maßnahmen ergreifen: von der Einführung neuer Technologien wie Post-Quanten-Verschlüsselung bis hin zur Stärkung ihrer Teams gegen KI-basierte Angriffe.

dSPACE fährt allein bei der Mail-Security mehrgleisig und nutzt verschiedene Schutzmaßnahmen. So setzt das Unternehmen zum Beispiel auf ein von einem Mitarbeiter entwickeltes Automatisierungstool für Rückmeldungen aus dem Sicherheits-Schwachstellenscan. „Da die technischen Meldungen oft zu Rückfragen und damit zu Verzögerungen führten, wird das Tool nun durch die Integration von KI optimiert", so Dominik Schopny, der sich in seiner durch dSPACE betreuten Bachelorarbeit mit der Thematik beschäftigt hat. In Zukunft werde ein Chatbot die benötigten Informationen automatisch in verständlicher, zielgruppengerechter Ansprache an die Empfänger versenden.

Mit sogenannten „Honeypots" hat sich dSPACE-Mitarbeiter Alexander Manzey in seinem Bachelorprojekt auseinandergesetzt. Diese digitalen Lockvögel sollen Cyberkriminelle anlocken und in die Irre führen. Dafür simulieren Honeypots unter anderem Daten, die für typische Angreifer interessant sind. „Das kann beispielsweise das vermeintliche Backup einer Personaldatenbank sein. Damit werden potentielle Cyberkriminelle von den wichtigen Produktivsystemen abgelenkt und es bleibt mehr Zeit, um auf die Bedrohung zu reagieren", so Manzey. Mit KI könne die Simulation weiter verbessert und automatisch aktualisiert werden. I