Gesamtverband der Deutschen Versicherungswirtschaft e. V.

CYBER SICHER

Eine Initiative der deutschen Versicherer.

Report

Cyberrisiken im produzierenden Gewerbe

GDV DIE DEUTSCHEN VERSICHERER

Methodik: Das haben wir getestet

Zur Bewertung der Cyberrisiken und der IT-Sicherheit des produzierenden Gewerbes hat der GDV im Jahr 2020 drei Untersuchungen mittelständischer Unternehmen aus fünf Branchen durchgeführt:

Elektro | Chemie | Kunststoff-verarbeitung | Maschinen-bau | Lebens-mittel

- Die **Forsa** Gesellschaft für Sozialforschung und statistische Analysen mbH befragte aus jeder der fünf Branchen jeweils 100 für die Internetsicherheit zuständigen Mitarbeiter.
- Der **Hacker und IT-Sicherheitsexperte Michael Wiesner** prüfte die technische und organisatorische IT-Sicherheit von 40 freiwillig teilnehmenden Mittelständlern aus dem produzierenden Gewerbe, unter anderem griff er die Unternehmen dabei mit Phishing-Mails an.
- Die **PPI AG** analysierte die Sicherheit der IT-Systeme von jeweils rund 500 Unternehmen der genannten Branchen. Dabei erfasst und bewertet sie mit dem Analyse-Tool **Cysmo** alle öffentlich einsehbaren Informationen aus Sicht eines potentiellen Angreifers. Zur Analyse gehört außerdem eine Suche nach Unternehmensdaten im Darknet.

Die Grafiken in diesem Report sind entsprechend gekennzeichnet.

Über die Initiative

Mit der Initiative CyberSicher sensibilisieren die Versicherer für die Gefahren aus dem Cyberspace und zeigen, wie sich kleine und mittlere Unternehmen schützen können. Dabei nimmt die Initiative auch die Cyberrisiken einzelner Branchen unter die Lupe.

CYBER@SICHER

Eine Initiative der Deutschen Versicherer.

Cyberrisiken im produzierenden Gewerbe

Oft im Fadenkreuz, zu selten vorbereitet

Kleine und mittelständische Unternehmen des produzierenden Gewerbes gelten oft als Hidden Champions: Egal ob im Maschinenbau, der Elektrotechnik oder im Bereich der Lebensmittel stellen sie weltweit begehrte Waren her. Dass sie dadurch für Hacker besonders interessant sind, ist vielen nicht bewusst. Die Folgen können buchstäblich vernichtend sein.

Ein Freitag im Mai 2019. Als Nesa Meta seinen Rechner starten will, merkt er, dass etwas nicht stimmt. „Wir haben die Systeme hochgefahren, dann kam schon die Meldung der Hacker“, erinnert sich der damalige Geschäftsführer des Schweizer Fensterherstellers Swisswindows. Die unbekannten Angreifer hatten alle 120 Server des Unternehmens mit Hilfe eines berüchtigten Verschlüsselungstrojaners gekapert. „Der Ryuk-Trojaner hat uns erwischt“, sagt Meta. Und zwar so richtig. Die rund 170 Mitarbeiter des Mittelständlers können keine E-Mails mehr verschicken, keine Kundentermine mehr einsehen und die Produktion liegt brach. Umgerechnet 650.000 Euro in Bitcoins soll die Firma zahlen, damit die Hacker die Systeme freigeben.

Doch ein Lösegeld kommt für das Management nicht in Frage. „Uns war sofort klar, dass wir mit Tätern nicht verhandeln wollen“, erzählt Meta. Auch die inzwischen eingeschalteten Sicherheitsbehörden hätten ihnen von einer Lösegeldzahlung abgeraten, sagt Meta.

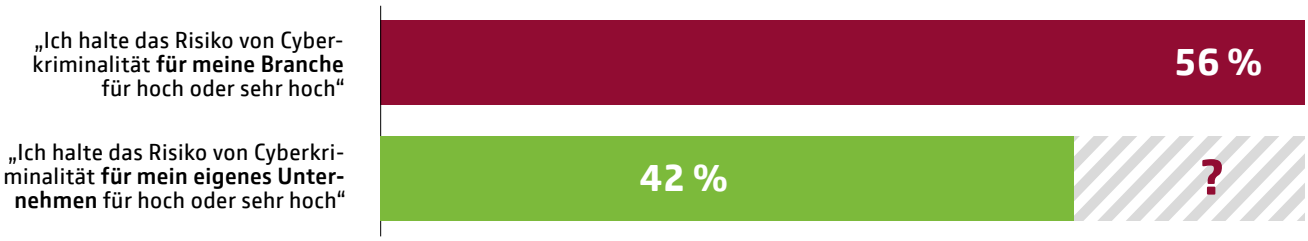
Was folgt, ist eine Betriebsunterbrechung von mehr als einem Monat. Weil auch die Backups fast vollständig verschlüsselt sind, müssen alle Systeme von Spezialisten neu aufgesetzt werden. Die Stammdaten sind größtenteils verloren: Kundendaten, Maschinendaten, Verträge – all das müssen die Mitarbeiter aufwendig von Hand neu eingeben. Doch damit ist der Alptraum nicht zu Ende. Nur wenige Kunden hätten Verständnis für die dramatische Lage gezeigt, berichtet Meta. So gesellen sich zu den Kosten für die Wiederherstellung der Systeme und zum Produktionsausfall auch Vertragsstrafen in erheblicher Größenordnung. „Durch den Angriff ist uns ein millionenschwerer Schaden entstanden.“ Zu viel für den Mittelständler. „Der Cyberangriff hat uns die Existenz genommen.“ Rund sieben Monate nach der Attacke meldet das Unternehmen Konkurs an. →

Verdrängtes Risiko – das kann teuer werden

Das Beispiel des Schweizer Fensterherstellers ist drastisch – und es macht deutlich, wohin ein erfolgreicher Cyberangriff im schlimmsten Fall führen kann. Umso beunruhigender, wie das produzierende Gewerbe in Deutschland mit der Bedrohung durch Cyberkriminalität umgeht. Nach einer Forsa-Umfrage im Auftrag des GDV ist sich eine Mehrzahl der kleinen und mittelgroßen Unternehmen in diesem Sektor zwar grundsätzlich der Gefahr bewusst, die von Hackern ausgeht: 56 Prozent schätzen sie als hoch bis sehr hoch ein. Wenn es jedoch um den eigenen Betrieb geht, sind viele der 500 befragten Entscheider aus Maschinenbau, Elektro-, Chemie-, Lebensmittelindustrie sowie der Kunststoffverarbeitung wesentlich zuversichtlicher: Für sich selbst stufen nur noch 42 Prozent das Risiko einer Cyberattacke als sehr hoch beziehungsweise hoch ein (siehe Grafik).

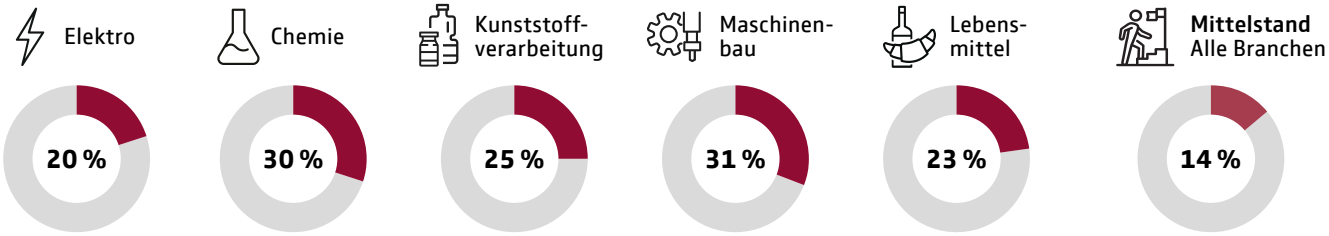
Das Risiko ist da, aber mein Unternehmen wird es schon nicht treffen. Wie kommen die Verantwortlichen darauf? Hier spielen vor allem zwei Argumente eine Rolle. Zum einen meinen die Verantwortlichen, ihre Computersysteme umfassend gegen Cyberangriffe geschützt zu haben. Zum anderen halten sich viele für zu klein und unbedeutend, um für Hacker interessant zu sein. Insbesondere die letztgenannte Einschätzung ist für Sicherheitsexperten bestenfalls leichtsinnig. „Hochprofessionelle Angriffe von Cyberkriminellen mit Ransomware etwa, Verschlüsselung und Diebstahl von Daten und Firmengeheimnissen und deren Verkauf oder Veröffentlichung sind eine reale Gefahr geworden“, sagt Arne Schönbohm, Präsident des Bundesamts für Sicherheit in der Informationstechnik (BSI). Nach Aussage des BSI, der Cybersicherheitsbehörde des Bundes, werden auch kleine und mittelständische Unternehmen Opfer von Cyberangriffen. Vor allem dann, wenn sie über gefragte Alleinstellungsmerkmale im Markt verfügen – etwa Maschinenbauer, die spezielle Komponenten herstellen. Das belegt auch die Forsa-Umfrage: Während jedes vierte

Die Einschätzung des eigenen Risikos wirft Fragen auf



Das produzierende Gewerbe ist ein beliebtes Ziel von Cyberkriminellen

Wurde Ihr Unternehmen durch Cyberangriffe geschädigt?



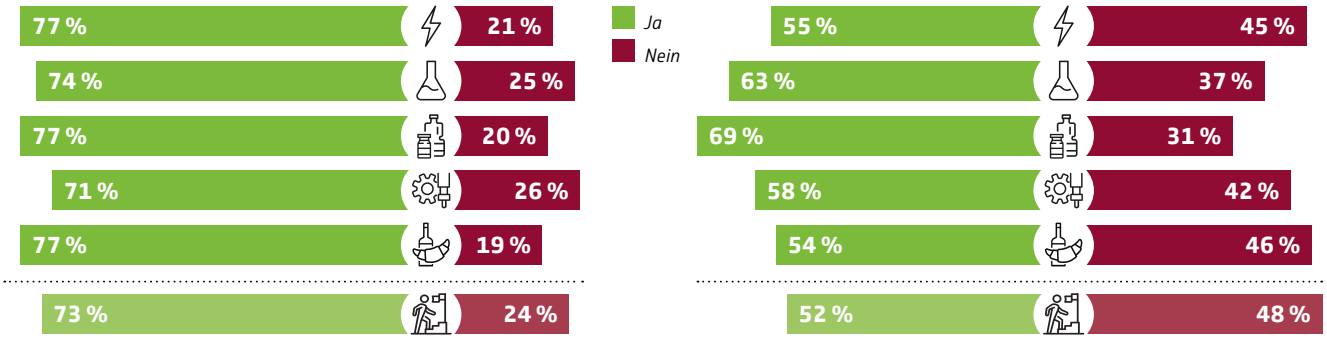
Quelle: Forsa

Viele sehen sich gut vorbereitet …

Hat Ihr Unternehmen ausreichende Maßnahmen zum Schutz gegen Internetkriminalität ergriffen?

… sind es aber im Ernstfall nicht

Haben Sie ein schriftliches Notfallkonzept und/oder eine entsprechende Vereinbarung mit Ihrem IT-Dienstleister?



Unternehmen mindestens einen Angriff erlebt hat, ist es im Maschinenbau und in der Chemieindustrie beinahe jedes dritte (siehe Grafik).

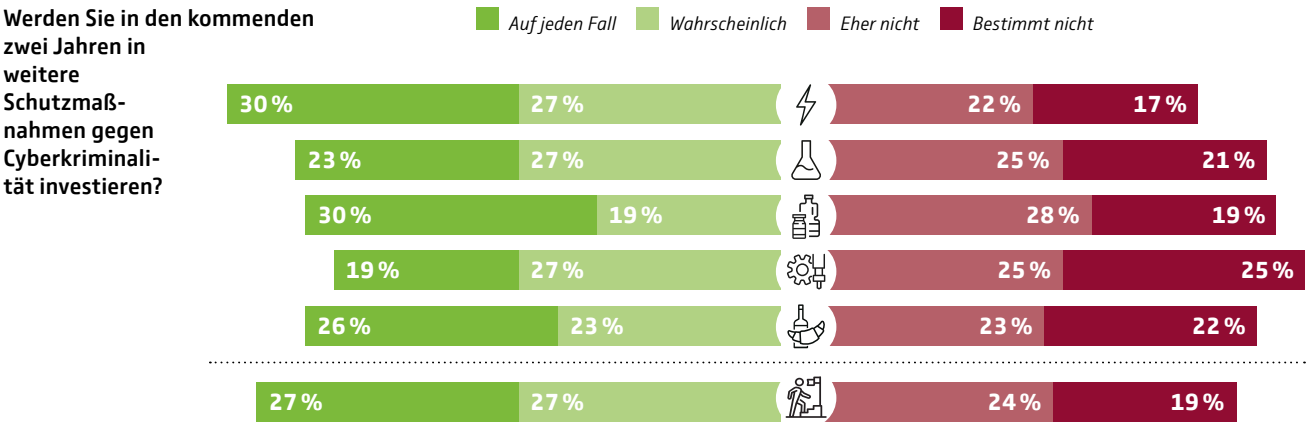
Der Trugschluss, nicht groß oder spannend genug für Hacker zu sein, kann mindestens sehr teuer werden. Dabei muss es nicht so dramatisch enden wie im Fall von Swisswindows. Doch bereits eine Woche Betriebsunterbrechung kann bei einem produzierenden Mittelständler schnell zu finanziellen Schäden in fünfstelliger Höhe führen – mindestens. Folgekosten für die Wiederherstellung der Daten, Rechtsberatung und Krisenkommunikation hinzugerechnet, kann sich der Schaden leicht verdreifachen. Das Bundeskriminalamt (BKA) und der IT-Branchenverband Bitkom beziffern die Schäden durch Hacker in der deutschen Wirtschaft auf hochgerechnet 103 Milliarden Euro (2019). Gegenüber dem Vorjahr sei dies nahezu eine Verdopplung, schreibt das BKA in seinem Lagebild Cybercrime.

Auch die Versicherer beobachten einen Trend zu höheren Schäden durch Cyberkriminalität. In einer aktuellen Analyse hat der Industrieversicherer AGCS kürzlich mehr als 1.700 Schadenmeldungen bei mehreren Versicherern über einen Zeitraum von fünf Jahren ausgewertet. Demnach lag der Gesamtschaden in der Cyberversicherung zwischen 2015 und 2020 bei 660 Millionen Euro, mit jährlich steigender Tendenz. Der weit überwiegende Teil (85 Prozent) geht auf kriminelle Hacker zurück. Ein weiteres Indiz dafür, wie dynamisch sich die Cyberkriminalität entwickelt: Das BSI zählt binnen eines Jahres mehr als 117 Millionen neue Schadprogramme, das entspricht rund 320.000 pro Tag.

Gut geschützt – IT-Experten sehen das anders

Ist das produzierende Gewerbe angesichts dieser wachsenden Bedrohung also wirklich so gut geschützt, wie die Entscheider meinen? Drei von vier sind der Auffassung, in ausreichendem Maße in den Schutz vor Internetkriminalität investiert zu haben (siehe Grafik). Auch ihre Auskünfte in der Forsa-Studie zu Sicherheitsmaßnahmen (siehe Seite 24 ff.) legt diesen Schluss zunächst nahe. Demnach machen viele Mittelständler vieles richtig: Sie vergeben Administratoren-Rechte nur an wenige Mitarbeiter, spielen automatisch Sicherheitsupdates ein. Sicherungskopien werden wöchentlich erstellt und ohne Netzzugang aufbewahrt, damit sie bei einem Angriff nicht in Mitleidenschaft gezogen werden. Doch nur eine knappe Mehrheit hat ein schriftliches Konzept für den Notfall in der Schublade oder einen externen Dienstleister damit betraut (siehe Grafik). Und bei allen technisch und administrativ aufwendigen Vorkehrungen – oft kommen die Hacker auf den vermeintlich einfachsten Wegen ins System: über E-Mails. →

Geringe Investitionsbereitschaft in IT-Sicherheit



→ So verschafften sich die Kriminellen mit weitem Abstand am häufigsten über das Mailsystem Zugang zu ihren Opfern (siehe Seite 16).

Auch Emotet, für das BSI bis zu ihrer Zerstörung Anfang 2021 die gefährlichste Schadsoftware der Welt, fand ihren Weg per Mail in die Firmensysteme. Diese Funktionsweise ist mit Emotet aber nicht verschwunden, sondern wird weiter genutzt: Öffnet der Nutzer die Dateien im Anhang, ist es bereits zu spät: Das Programm kann weitere Schadsoftware nachladen und die Angreifer übernehmen die Kontrolle über die infizierten Rechner. Inzwischen nutzen die Kriminellen ihren Zugang nicht mehr nur, um Daten zu verschlüsseln und Lösegeld dafür zu verlangen, sondern immer häufiger auch um interne Informationen zu kopieren und zu stehlen. „Auch für KMU gilt deshalb: Voraussetzung einer erfolgreichen Digitalisierung ist die Informationssicherheit“, mahnt BSI-Chef Schönbohm.

Nicht zuletzt deshalb bewerten unabhängige IT-Sicherheitsexperten die Bemühungen der Unternehmen, sich gegen Cyberangriffe zu schützen, als unzureichend. Als Berater und so genannter White-Hat-Hacker prüft Michael Wiesner seit vielen Jahren die IT-Sicherheit in Unternehmen. Sein nüchternes Urteil: Die Firmen investieren weder finanziell noch personell merklich mehr in Cyberschutz. „Ich sehe keinen Kulturwandel“, sagt er. Defizite gibt es vor allem in Sensibilisierung gegen Phishing-Angriffe, wie er in einer aktuellen Untersuchung von 40 KMU des produzierenden Gewerbes für den GDV (siehe Seite 12) herausgefunden hat. Mit seiner Phishing-Mail kam er bei jedem zweiten Unternehmen an die Zugänge und Passwörter gleich mehrerer Mitarbeiter – in einem Unternehmen fielen sogar gleich dutzende Angestellte auf die Mail herein. Hinzu kommen demnach Sicherheitslücken in internen IT-Systemen sowie fehlendes Informationssicherheits- und Vorfallmanagement. Das durchschnittliche Sicherheitsniveau bewertet Wiesner als unzureichend, das resultierende Risiko, Opfer eines Angriffs zu werden, als mittel bis hoch. Laut Forsa-Studie will lediglich jeder zweite Betrieb den IT-Schutz in den kommenden zwei Jahren ausbauen (siehe Grafik). Für Wiesner ist das angesichts der dynamischen Entwicklung der Angriffe zu wenig. „Die Firmen tun das, was absolut notwendig ist – mehr aber auch nicht.“ ←

Was eine Cyberattacke kosten kann – und eine Cyberversicherung deckt

Musterszenario Ransomware:

Hacker attackieren mit einem Verschlüsselungs-Trojaner die IT-Systeme eines Maschinenbauers. Sie wollen die gesperrten Rechner erst wieder freigeben, wenn sie Lösegeld bekommen.

1 Angriff

Sämtliche Rechner und die vernetzten Produktionssysteme des Maschinenbauers sind ohne Funktion. Auf den Bildschirmen der Steuerungsrechner erscheint lediglich eine Nachricht der Erpresser.

2 IT-Forensik und Datenwiederherstellung

Nach Rücksprache mit Polizei und Staatsanwaltschaft zahlt das Unternehmen kein Lösegeld. IT-Spezialisten arbeiten mehrere Tage daran, den Trojaner von sämtlichen Systemen zu entfernen; anschließend müssen sie alle Daten aus den Backups wiederherstellen.

Kosten für IT-Forensik und Datenwiederherstellung: 40.000 Euro

3 Betriebsunterbrechung

Bis die Systeme wieder laufen, kann das Unternehmen nicht produzieren. Die Mitarbeiter aus Fertigung und Verwaltung bleiben zuhause.

Kosten für 5 Tage Betriebsunterbrechung: 45.000 Euro

4 Information von Kunden und Vertragspartnern

Die IT-Forensiker können nicht ausschließen, dass Daten nicht nur gesperrt, sondern auch entwendet wurden. In diesem Fall wären auch Betriebsgeheimnisse von Vertragspartnern betroffen, die vorsorglich informiert werden müssen.

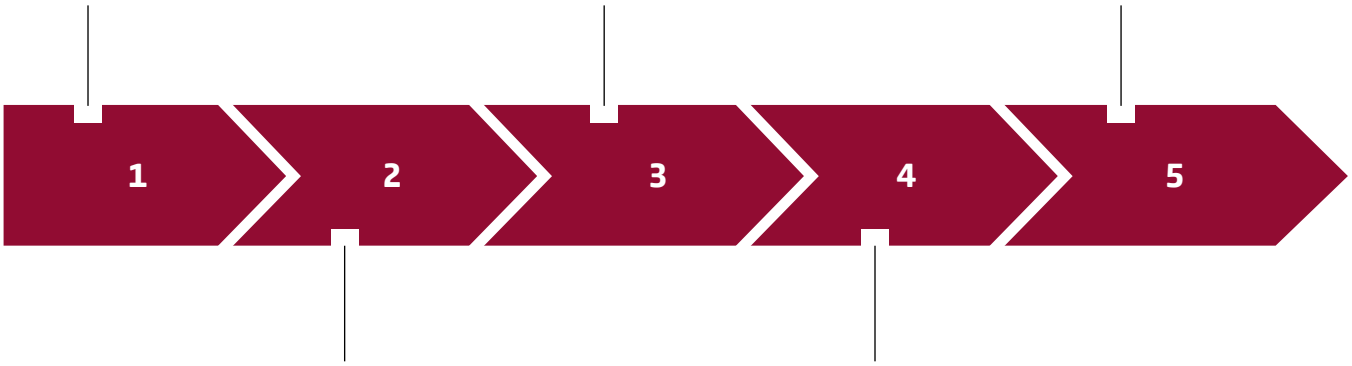
Informationskosten und Rechtsberatung: 20.000 Euro

5 Vertrauenskrise

Der bisher tadellose Ruf des Unternehmens nimmt in wichtigen Kundenbranchen Schaden; einige Kunden wenden sich vom Unternehmen ab, der Umsatz sinkt spürbar.

Krisenkommunikation: 30.000 Euro

Der Umsatzrückgang ist nicht gedeckt.



»Eine Cyberpolice ist dringend notwendig«

Gerhard Klein führt eine Druckerei in Saarbrücken. Im Herbst 2018 wird sein Unternehmen zum Ziel einer Ransomware-Attacke. Er zahlt 3.500 Euro an die Erpresser – als diese mehr Geld wollen, ändern Klein und sein Team die Taktik. Statt zu zahlen, versuchen Spezialisten gesperrte Daten wiederherzustellen. Wochenlang haben die Beschäftigten damit zu tun, verlorene Kundendaten, Rechnungen und auch die Lohnbuchhaltung wieder in den Griff zu bekommen.

Klein schaltet die Polizei ein und macht den Hackerangriff auf sein Unternehmen öffentlich. Zahlreiche Medien berichteten vom Schadensfall bei dem Mittelständler. Gerade dieser offene Umgang ist ungewöhnlich – viele Betroffene scheuen aus Sorge um den Ruf ihrer Firma davor zurück. Für Klein und sein Team ist der Schritt an die Öffentlichkeit bis heute richtig. Denn statt Häme erfuhren sie Verständnis. Statt Kritik an mangelhafter Cybersicherheit gab es aufmunternden Zuspruch.

Nach dem Schock und dem Schaden von rund 70.000 Euro rüstete Klein bei der Computersicherheit systematisch auf. Ein wichtiger Aspekt für ihn dabei: Das Team muss mitmachen. Denn alle technische Finesse nützt nichts, wenn die Beschäftigten sie im Alltag nicht zu nutzen wissen.

Und heute? Lässt die Wachsamkeit nach? Schleichen sich Nachlässigkeiten ein?

Herr Klein, inzwischen ist der Hackerangriff auf Ihr Unternehmen zwei Jahre her. Was ist von dem Schreck damals geblieben?

Wir sind heute natürlich wieder deutlich entspannter als in den ersten Monaten nach dem Angriff. Aber die Mitarbeiter sind dennoch sehr, sehr aufmerksam. Ein Beispiel: Ich habe immer noch sehr engen Kontakt zur Kriminalpolizei, die sich mit Cyberattacken beschäftigt. Da bekommen wir auch regelmäßig Warnungen über neue Bedrohungen, die ich an meine Mitarbeiter weiterleite. Und genauso regelmäßig fragen einige extra bei mir nach, ob diese Mail tatsächlich von mir kommt und ob sie das darin enthaltene Dokument wirklich öffnen dürfen.

Das ist ja vorbildlich. Führen Sie das auf den Schock damals zurück oder schulen Sie Ihre Beschäftigten einfach häufiger?

Wer einen solchen Angriff und die Folgen einmal miterlebt hat, ob nun als Mitarbeiter oder als Firmenchef, verfällt danach nicht wieder in Routine. Das ist, um es noch mal ganz deutlich zu sagen, ein dramatisches Ereignis. Insofern resultiert das beschriebene Verhalten sicher zu 80 Prozent aus dem heilsamen Schock von damals. Und ansonsten schulen wir stetig im Berufsalltag: Wie gehe ich mit Mails um? Wenn ich mir nicht sicher bin, wo eine Mail herkommt, wenn der Betreff seltsam aussieht, wenn mich irgendetwas stört, wird gelöscht. Das ist die Vorgabe.

Finden Sie das nicht übervorsichtig?

Nein, das ist nicht übervorsichtig. Vor kurzem habe ich selbst eine Mail gelöscht, die mir verdächtig vorkam, weil sie keinen Betreff hatte. Hinterher stellte sich heraus, sie war von einem Kunden. Gut, dann muss man eben telefonieren und der Kunde muss die Mail nochmal schicken. Aber es ist kein Grund für uns, unser Verhalten zu ändern. Sicherheit geht hier ganz klar vor.

Wie reagieren Kunden in einem solchen Fall?

Ich habe bisher noch keinen Kunden erlebt, der das nicht verstanden hat.

Zur Person

Gerhard Klein ist Geschäftsführer der Braun und Klein Siebdruck GmbH. Die digitale Welt ist ihm nicht fremd. Noch aus dem Informatik-Studium ist ihm die Sache mit den Einsen und den Nullen wohl vertraut. Und später im Beruf: Wohl kaum eine andere Branche hat sich durch die Digitalisierung so früh und nachhaltig verändert wie die Druckindustrie.

Apropos Kunden: Sie sind damals sehr offen mit dem Angriff umgegangen, haben Interviews gegeben, Vorträge gehalten. Haben Sie langfristig negative Reaktionen von Kunden erfahren?

Nein, wir haben bis heute keine negativen Erfahrungen gemacht. Die Menschen reagieren positiv, nach dem Motto: Wenn ein Unternehmen offen mit einem solchen Angriff umgeht, wird es diese Situation meistern. Die Kunden haben uns von Anfang an Vertrauen entgegengebracht.

Führen Sie heute regelmäßig Schulungen Ihrer Mitarbeiter durch?

Schulungen in Form von Seminaren oder Veranstaltungen führen wir nicht durch. Unser Betrieb hat 27 Leute und nur etwa die Hälfte arbeitet mit dem Internet. Aber: Wir sprechen unsere Mitarbeiter im Arbeitsalltag immer wieder auf das Thema IT-Sicherheit an und sensibilisieren sie dafür, wie wichtig das ist.

Was ist bei Ihnen persönlich vom Angriff geblieben?

In jedem Fall habe ich eine gewisse Stressresistenz entwickelt. Als Unternehmer ist es ja so, dass man eben etwas unternimmt, wenn es ein Problem gibt. Nach der Cyberattacke konnte ich aber nichts tun, sondern musste mich darauf verlassen, dass die Spezialisten das Richtige unternehmen. Ich war also gezwungen, eine größere Gelassenheit zu entwickeln. Und mehr zu kommunizieren.

Die Cyberattacke hat Ihre Art, das Unternehmen zu leiten, verändert?

Ja. Damals haben wir als Geschäftsführung gelernt, mehr mit unseren Mitarbeitern zu reden. Kommunikation mit jeder Mitarbeiterin, mit jedem Mitarbeiter ist gerade in Krisenzeiten ein wichtiges Element. Nur so kann ich dafür sorgen, dass sie das Vertrauen in die Firma und in die Geschäftsführung behalten. Das heißt, ich erkläre meine Entscheidungen heute ausführlicher als früher.

Der Hackerangriff erwischte Sie damals in einer Phase, in der Sie noch keine Cyberversicherung hatten.

Wir hatten damals bereits ein Angebot vorliegen und dann kam der Angriff. Heute muss man sagen: Die Police hätte uns ohnehin nicht viel geholfen, weil dort Schäden bis maximal 50.000 Euro abgedeckt gewesen wären. Mit dem Wissen von heute ist das natürlich viel zu wenig.

Eine Cyberversicherung hilft also nicht?

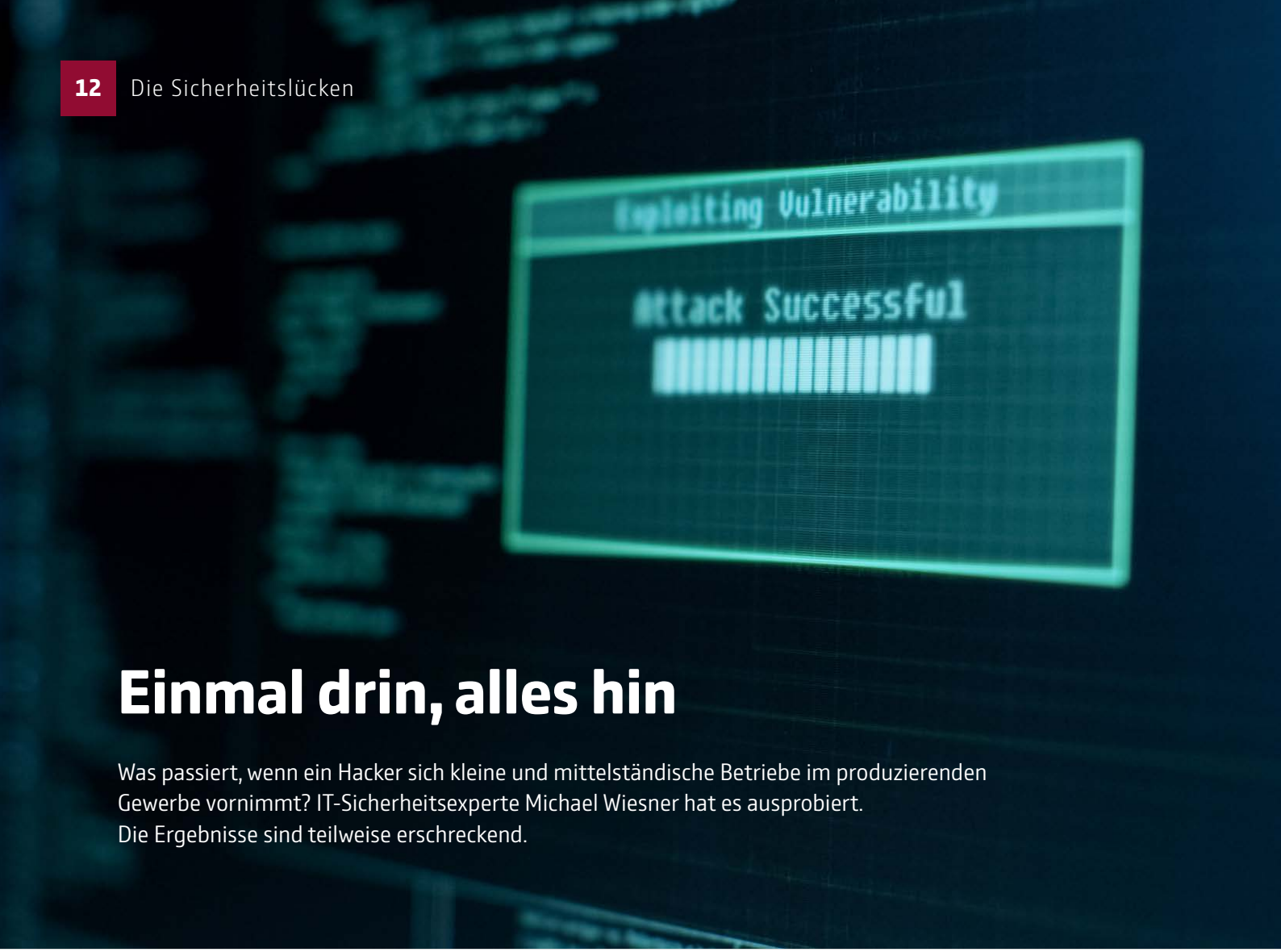
Doch, natürlich. Nach der Erfahrung, die wir damals mit der Ransomware-Attacke machen mussten, kann ich Unternehmen nur dringend empfehlen, sich mit einer solchen Police zu beschäftigen. Das ist wie eine Elementarschadenversicherung fürs Haus – aus meiner Sicht unbedingt notwendig. Das Thema Cyberversicherung sind wir angegangen, sobald wir nach dem Angriff wieder einen klaren Kopf hatten. Inzwischen haben wir eine passende Versicherung gefunden und abgeschlossen.

Und die Deckungssumme reicht?

Die aktuelle Police deckt Schäden bis hin zur Abwicklung des Unternehmens ab.

Um eine solche Police zu bekommen, müssen Unternehmen ja bestimmten Sicherheitsanforderungen genügen.

Natürlich konnten wir einen Plan für unsere IT-Sicherheit vorlegen, weil wir uns ja gerade ausführlich damit auseinandergesetzt hatten. Unternehmen, die noch nicht so weit sind, bekommen von den Versicherern Hilfe angeboten, um die Kriterien zu erfüllen.



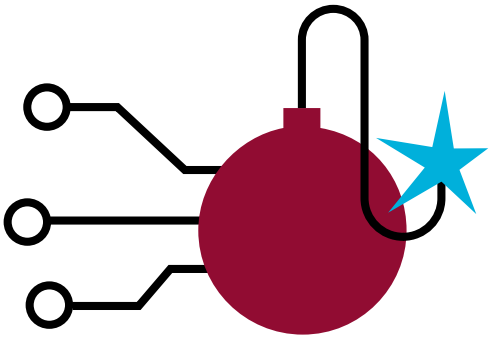
Einmal drin, alles hin

Was passiert, wenn ein Hacker sich kleine und mittelständische Betriebe im produzierenden Gewerbe vornimmt? IT-Sicherheitsexperte Michael Wiesner hat es ausprobiert. Die Ergebnisse sind teilweise erschreckend.

Wenn die Maschine die Fertigung selbst organisiert und intelligente Roboter Menschen bei der Fertigung zur Hand gehen, ist das Industrie 4.0. Und intelligente Lieferketten, die Material just in time dahin bringen, wo es benötigt wird, sind im produzierenden Gewerbe zunehmend so selbstverständlich wie intelligente Steuerketten, die wissen, wann sie das nächste Mal gewartet werden müssen. Doch wie gut sind die Maschinendaten vor Hackerangriffen geschützt? Sind Produktionsbetriebe bei der IT-Sicherheit genauso innovativ wie bei der Fertigung?

„Sagen wir es mal so: Die Eigenwahrnehmung in puncto Informationssicherheit unterscheidet sich bei sehr vielen Mittelständlern ganz eklatant von der Realität“, sagt Michael Wiesner. Als so genannter White-Hat-Hacker wird er von Unternehmen beauftragt, um in simulierten Angriffen ihren tatsächlichen Schutz zu prüfen und auf Sicherheitslücken aufmerksam zu machen. Für den Gesamtverband der Deutschen Versicherungswirtschaft hat er 40 kleine und mittelständische Unternehmen aus dem produzierenden Gewerbe einem mehrstufigen Stresstest unterzogen. „Das Ergebnis war insgesamt nicht schön, aber es hat mich auch nicht überrascht“, berichtet der IT-Sicherheitsexperte, der seit 25 Jahren im Geschäft ist.

„Nicht schön“ – das bedeutet im Klartext: Bei mehr als der Hälfte der Firmen konnten Wiesner und sein Team die Systeme hacken. Spielend leicht hätten sie Daten manipulieren und Maschinen übernehmen können. Ein verheerendes Fazit – vor allem, weil sich die Unternehmen freiwillig für den Test gemeldet hatten. Sie waren also vorgewarnt und hätten vorbereitet sein können. Dabei verhielten sich die IT-Sicherheitsspezialisten wie echte Cyberkriminelle, wenn sie es auf ein ganz bestimmtes Ziel abgesehen haben: Sie suchen den schnellsten Weg ins Herz der Systeme. Stufe



Eins ist zunächst einmal ganz analog. Wie ist der Eingangsbereich des Unternehmens gesichert? Gibt es dort Möglichkeiten, leicht ins Netzwerk oder an Passwörter von Angestellten zu gelangen? In einer zweiten Stufe schickten die Experten Phishing-Mails an die ganze Belegschaft. Waren sie dann erst einmal in ein System eingedrungen, erfolgte der Angriff auf alle möglichen Datenbanken und Maschinensteuerungen der Unternehmen.

Unternehmen sind Eindringlingen schutzlos ausgeliefert

Die größte Schwachstelle ist noch immer der Mensch. Allein über Phishing-Mails und gefälschte Webseiten gelangte Wiesner an die Zugangsdaten von 200 Mitarbeiterinnen und Mitarbeitern aus 19 Firmen. In sieben weiteren Unternehmen gaben Angestellte zwar keine Daten preis – dafür klickten sie aber Links an, über die echte Cyberkriminelle leicht Schadsoftware im Firmensystem hätten installieren können. Eigentlich eine alarmierende Bilanz. Aber: „Dass Phishing so erfolgreich war, hat die wenigsten Unternehmen überrascht“, berichtet Wiesner von der Reaktion der Firmen.

Geschockt zeigten sich einige Firmen immerhin über das, was dann folgte. „Wenn wir einmal in ein Netzwerk eingedrungen waren, konnten wir dort praktisch machen, was wir wollten“, beschreibt der White-Hat-Hacker. Das heißt: Wenn ein Angreifer einmal drin ist, geben die Systeme auch dann keine Warnung aus, wenn Anomalien auftreten. „Nicht ein Unternehmen verfügte über reaktive Maßnahmen.“

Angesichts solch eklatanter Sicherheitslücken treten die wenigen positiven Ergebnisse der Untersuchung in den Hintergrund. So war die „physische Sicherheit“ bei den meisten Mittelständlern weitgehend gegeben. Netzwerk-Stecker in der Lobby oder ähnliche Einfallstore waren überwiegend gut gegen Eindringlinge abgeschirmt. Ebenfalls nur ein kleiner Lichtblick: In einigen Unternehmen gab es getrennte Kreisläufe für unterschiedlich sensible Bereiche. Im Fall eines Hackerangriffs kann das von existentieller Bedeutung sein. Gelingt es Cyberkriminellen etwa sich Zugriff auf den Mailserver zu verschaffen, könnten sie andernfalls nämlich Maschinen kapern und schlimmstenfalls die Produktion komplett stoppen. Allerdings: „Die Segmentierung der Sicherheitskreisläufe verbessert sich nur langsam“, sagt IT-Sicherheitsexperte Wiesner. „Inzwischen sehen wir sie immerhin in 20 bis 30 Prozent der Unternehmen.“

Drei zentrale Punkte machen Unternehmen schwach

Insgesamt bemängelt Wiesner die Geschwindigkeit, mit der sich der Sinneswandel in den Unternehmen vollzieht. Für ihn sind es drei zentrale Knackpunkte, die zu den wenig erfreulichen Ergebnissen der Studie führen: unklare Zuständigkeiten, mangelhafte Risikoeinschätzung und fehlende Ressourcen. Wenn es darum geht, wer für die Datensicherheit in der Produktion zuständig ist, schieben sich die Abteilungen nach Erfahrung des Experten die Verantwortung zu häufig gegenseitig zu. Das liege nicht zuletzt an der zunehmenden Digitalisierung der Produktionsprozesse. IT und produktionsnahe Steuerung verschmelzen also immer stärker. „In der Praxis führt das oft zu einem Kompetenzvakuum“, erläutert Wiesner. „Die IT fühlt sich nicht für die Maschinensicherheit verantwortlich und die operativen Mitarbeiter fühlen sich nicht als IT-Spezialisten.“ →

→ Doch sind es längst nicht die Mitarbeitenden, die mit ihrem Verhalten für die in vielen Betrieben noch immer mangelhafte IT-Sicherheit sorgen. „Dem Management fehlt nach wie vor zu häufig die Expertise, um die richtigen Schritte in der IT-Sicherheit zu gehen“, urteilt Wiesner. Teils mangele es bei den Verantwortlichen an Vorstellungskraft, wie kreativ Cyberkriminelle sind. Und diese Fehleinschätzung bestehender Risiken hat nach Erfahrung des Experten wiederum fatale Folgen für das IT-Budget – personell wie finanziell. „Wenn Sicherheitslücken bestehen, hat das nicht zwingend mit einer mangelnden Kompetenz der IT-Mitarbeiter zu tun – sondern vielmehr mit fehlendem Personal und einer zu geringen finanziellen Ausstattung.“

Bei den untersuchten Unternehmen kommt im Schnitt eine IT-Kraft auf 87 Mitarbeitende. Für Mittelständler mit 200 Beschäftigten bedeutet das, sie haben 2,2 Angestellte, die sich um die gesamten IT-Systeme des Betriebes inklusive des Maschinenparks kümmern und alles am Laufen halten müssen – für Prävention und die ständige Verbesserung der IT-Sicherheit bleibt dann kaum noch Zeit. Je kleiner das Unternehmen, desto größer übrigens das Problem: Ein Drittel der untersuchten Betriebe beschäftigt gar keine eigenen IT-Kräfte – alle diese Firmen haben weniger als 100 Mitarbeiter.

Zu oft steht Sicherheit nur auf dem Papier

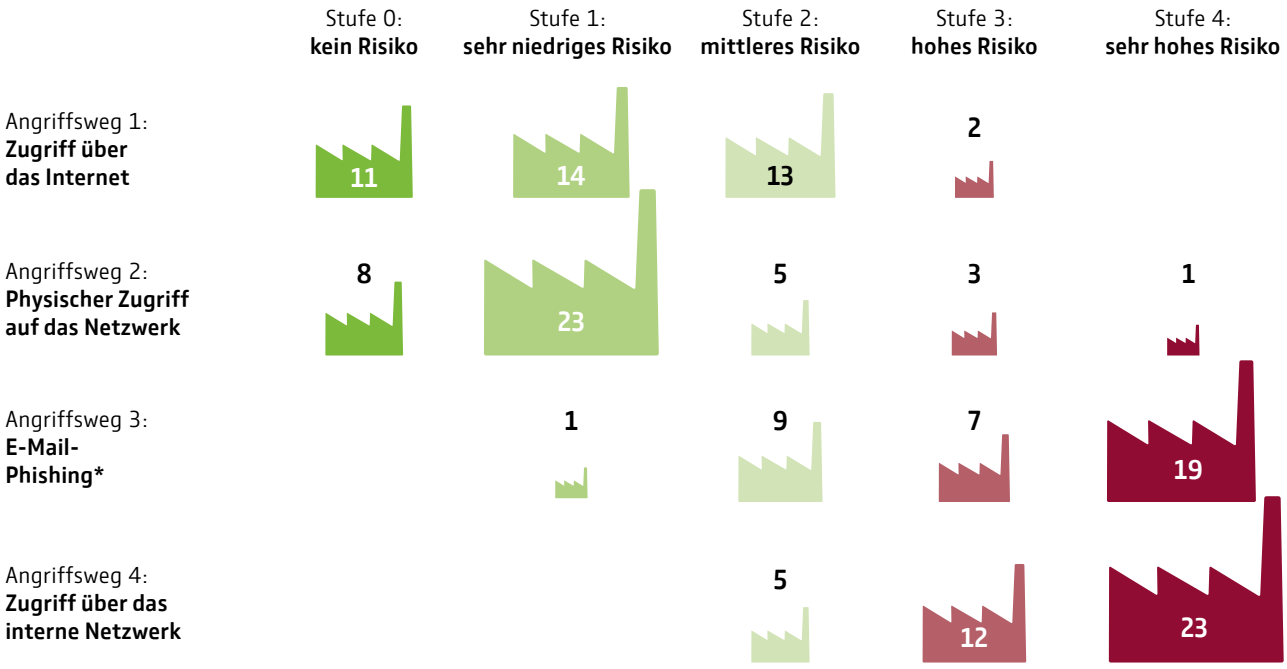
Was können kleine und mittelständische Unternehmen tun, um der wachsenden Gefahr durch Cyberangriffe zu begegnen? Sie müs-

„Wenn Sicherheitslücken bestehen, hat das nicht zwingend mit einer mangelnden Kompetenz der IT-Mitarbeiter zu tun – sondern vielmehr mit fehlendem Personal und einer zu geringen finanziellen Ausstattung.“

Michael Wiesner, IT-Sicherheitsexperte

Der Weg ins IT-Netzwerk führt über die Mitarbeiter

So waren die Teilnehmer am IT-Sicherheitscheck gegen die Angriffswege von Cyberkriminellen geschützt



* Vier Unternehmen haben am Phishing-Test nicht teilgenommen

sen IT-Sicherheit leben – und das bedeutet, IT-Sicherheit muss Managementaufgabe sein, meint White-Hat-Hacker Wiesner. Ein so genanntes Information Security Management System (ISMS) kann hier ein sinnvolles Instrument sein. Ein solches Konzept definiert Regeln und Methoden, um die Informationssicherheit in einem Unternehmen zu gewährleisten. Ganz zentral dabei: Es verfolgt einen Top-Down-Ansatz ausgehend von der Unternehmensführung.

Ein ISMS nützt allerdings wenig, wenn es nur auf dem Papier steht, wie auch die aktuelle Untersuchung zeigt. Nach eigenen Angaben besitzen nämlich sechs der 40 Unternehmen Grundzüge eines ISMS, eines betreibt sogar ein vollständiges. „Ausgerechnet eines dieser Unternehmen war es, in das wir am leichtesten eindringen konnten“, sagt Wiesner.

Ob mit ISMS oder ohne – schon mit eigentlich selbstverständlichen technischen Maßnahmen lässt sich eine verbesserte Sicherheit gegen Hacker erzielen. „Zum Beispiel, indem Unternehmen ihre Betriebssysteme aktuell halten, regelmäßig Sicherheitsupdates einspielen und eine Zwei-Faktor-Authentifizierung für ihre Mitarbeitenden einführen“, zählt Wiesner auf. Und auch wenn die finanziellen Mittel gerade in kleineren Produktionsbetrieben endlich seien, sei IT- und Maschinensicherheit gut umsetzbar: „Ein wichtiger Faktor neben mehr Geld und mehr Personal und Konzepten wie einem Informationssicherheitsmanagementsystem ist: die Kommunikation.“

Hier sind alle Mitarbeitenden gefragt. Regelmäßige Phishing-Kampagnen beispielsweise könnten Belegschaften für die Gefahren, die dort lauern, sensibilisieren. „Und: Geschäftsführung und IT-Verantwortliche müssen mehr miteinander reden.“ Managemententscheidungen können nur so gut sein, wie die Informationen, auf denen sie beruhen. „In zu vielen Unternehmen lebt noch das Klischee von den IT-Mitarbeitenden, die im Keller sitzen und Pizza bestellen und ansonsten die Bürotür am liebsten geschlossen halten.“

Gefährliche Post

Das E-Mail-Postfach ist für viele Unternehmen die wichtigste digitale Schnittstelle zu Kunden und Lieferanten. Für Hacker ist dies der ideale Angriffspunkt: Sie bringen mit immer raffinierteren Methoden ihre Opfer dazu, Spam E-Mails zu öffnen – und legen mit ihrer Schadsoftware nicht nur die IT-Systeme, sondern ganze Betriebe lahm. Manche schaffen es sogar, die Zugangsdaten von Mitarbeitern abzufragen und können so das ganze IT-Netzwerk nicht nur sperren, sondern fast nach Belieben – und häufig unbemerkt – kontrollieren. Die dritte Gefahr schließlich geht über den Mail-Eingang hinaus: Bei der privaten Nutzung dienstlicher Accounts können Mail-Adressen und Passwörter ins Darknet geraten und werden Hackern somit auf dem Silbertablett präsentiert.

Früher war Spam leicht zu erkennen: unseriöse Absender, vermeintliche Gewinn-Überraschungen oder kuriose Satzstellungen. Doch diese Zeiten sind vorbei. Und falls solche E-Mails es durch den Spam-Filter schaffen, liegt es an den Empfängern, sie als unseriös einzustufen und in den Papierkorb zu verschieben. Hacker finden jedoch immer wieder ausgefeilte Methoden, Menschen so zu manipulieren, dass sie Schadsoftware herunterladen oder Passwörter herausgeben. Mit zuvor gesammelten Daten eines Unternehmens können sie ihren Angriff als seriöse Mail ausgeben und nutzen so die menschliche Neugierde aus. Social Hacking nennt sich diese geschickte Manipulation.

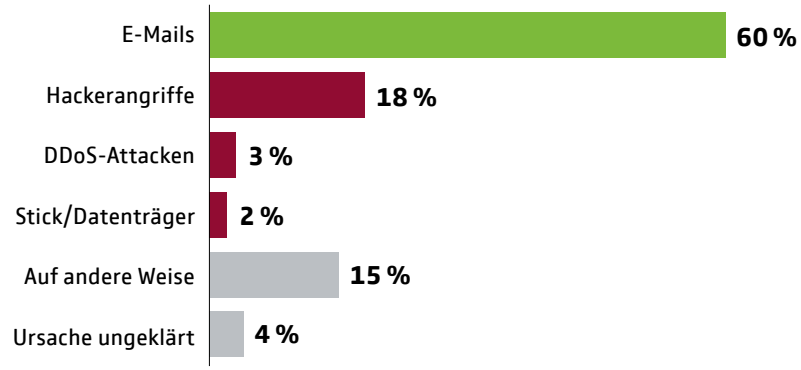
So hat es auch Michael Wiesner gemacht. Der IT-Sicherheitsberater und White-Hat-Hacker hatte vom GDV den Auftrag erhalten, Mittelständler aus dem produzierenden Gewerbe auf Herz und Nieren zu prüfen (siehe Seite 12). Sein Phishing-Trick: Er lud die Belegschaft ausgerechnet zu einer angeblichen IT-Sicherheitsschulung ein, zu der sich die Mitarbeiter mit ihrem Windows-Anmeldedaten einloggen sollten. So kam er an die Zugangsdaten von 200 Angestellten aus 19 Firmen.

Weil sich zu viele Menschen nahezu blind auf Firewall und Virenscanner verlässt, ist es keine Überraschung, dass fast zwei Drittel aller erfolgreichen Hacker-Angriffe ganz einfach am Mail-Postfach ansetzen – denn die Schwachstelle Mensch lässt sich noch zu leicht überlisten. „Die technischen Hilfsmittel können den gesunden Menschenverstand und eine gewisse Skepsis nicht ersetzen, Unternehmen müssen ihre Mitarbeiter daher besser auf die Gefahren aus dem Netz vorbereiten“, sagt Peter Graß, Cyberversicherungsexperte des GDV. „Cyberangriffe sind selten ausgefeilte Angriffe durch Netzwerklücken, viel öfter entstehen Schäden durch Menschen, die unbedacht eine infizierte E-Mail öffnen.“ Deswegen ist es umso wichtiger, Mitarbeiterinnen und Mitarbeiter entsprechend zu schulen und Richtlinien zur Nutzung von E-Mail festzulegen.

Vor allem in Bezug auf die private Nutzung des dienstlichen Mail-Accounts sollte es verbindliche Regelungen geben, denn viele sind sich der Gefahr bei privater Nutzung offenbar nicht bewusst: Bei einer Prüfung von mehr als 2.500 Mittelständlern aus dem produzierenden Gewerbe mit Hilfe des Analyse-Tools Cysmo konnten von knapp 1.000 Unternehmen Daten im Darknet gefunden werden, darunter fast →

Die Einfallstore

Erfolgreiche Cyberangriffe erfolgten durch … [1]

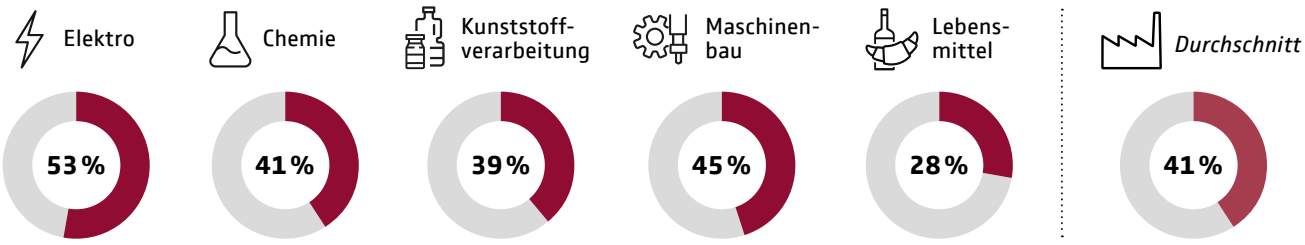


Quelle: Forsa

1 Mehrfachnennungen möglich

Sensible Daten im Darknet

Anteil der Unternehmen, von denen Daten im Darknet zu finden waren.



Zum Vergleich: **Mittelstand** branchenübergreifend: **53 %**

Quelle: Cysmo

„Regelmäßige Schulungen und verbindliche Vorsichtsmaßnahmen sind unverzichtbar, wenn Unternehmen nicht riskieren wollen, dass Adressen und Passwörter im Darknet landen oder Spam geöffnet wird."

Peter Graß, GDV-Cyberversicherungsexperte

→ 35.000 Mail-Adressen mit den dazugehörigen Passwörtern.

Doch wie kommen die dienstlichen E-Mail-Adressen der Mitarbeiter überhaupt ins Darknet? Auch darauf geben die Daten Hinweise: Die Studie zeigt, dass Mitarbeiter ihre dienstlichen Mail-Adressen vielfach eben nicht nur dienstlich, sondern auch privat benutzen – und das nicht nur für Einkäufe in online Shops oder soziale Netzwerke wie Facebook. So manch einer scheut nicht davor zurück, sich mit seiner Dienstadresse in Dating-Portalen wie Badoo, Dating.de oder Fling zu registrieren. Seltener, aber beileibe kein Einzelfall ist auch die Anmeldung in Portalen für „Erwachsenenunterhaltung". Zu den gefundenen Rückzugsorten gehören hier zum Beispiel Brazzers oder Youporn. Durch diese fragwürdige private Nutzung der dienstlichen Mail-Adresse schleusen die Mitarbeiter möglicherweise sogar Daten ins Darknet, die von Hackern zur Erpressung genutzt werden können. „Private und berufliche Mail-Accounts und die entsprechenden Aktivitäten sollten immer strikt voneinander getrennt werden – dazu gehört auch, nicht ein und dasselbe Passwort für beide Accounts zu benutzen", warnt Graß. ←

So schützen Sie Ihr Unternehmen vor schädlichen E-Mails

Nur ein einziger falscher Klick auf einen verseuchten Mail-Anhang oder einen Link kann Ihre Unternehmens-IT lahmlegen. Wenn Sie Ihre Mitarbeiter regelmäßig für die Gefahren sensibilisieren und einige grundlegende Regeln für den Umgang mit E-Mails aufstellen, können Sie sich vor vielen Angriffen schützen.

1. Arbeiten Sie mit hohen Sicherheitseinstellungen
Nutzen Sie die Sicherheitseinstellungen Ihres Betriebssystems und Ihrer Software zu Ihrem Schutz. Im Office-Paket sollten zum Beispiel Makros dauerhaft deaktiviert sein und nur bei Bedarf und im Einzelfall aktiviert werden können – denn auch über diese kleinen Unterprogramme in Word-Dokumenten oder Excel-Listen kann sich Schadsoftware verbreiten.

2. Halten Sie Virenscanner und Firewall immer auf dem neuesten Stand
Die meisten schädlichen E-Mails können Sie mit einem Virenscanner und einer Firewall automatisch herausfiltern lassen. Wirksam geschützt sind Sie aber nur, wenn Sie die Sicherheits-Updates auch schnell installieren.

3. Öffnen Sie E-Mails nicht automatisch
Firewall und Virenscanner erkennen nicht alle schädlichen Mails. Öffnen Sie also nicht gedankenlos jede Mail in Ihrem Posteingang. Erster Schritt: Stellen Sie in Ihrem E-Mail-Programm die „Autovorschau" aus. So verhindern Sie, dass sich schädliche E-Mails automatisch öffnen und Viren oder Würmer sofort aktiv werden.

4. Vor dem Öffnen: Prüfen Sie Absender und Betreff
Cyberkriminelle verstecken sich gern hinter seriös wirkenden Absenderadressen. Ist Ihnen der Absender der E-Mail bekannt? Und wenn ja: Ist der Absender wirklich echt? Achten Sie auf kleine Fehler in der Schreibweise oder ungewöhnliche Domain-Angaben hinter dem @. In betrügerischen E-Mails ist auch der Betreff oft nur unpräzise formuliert, z. B. „Ihre Rechnung".

5. Öffnen Sie Links und Anhänge nur von wirklich vertrauenswürdigen E-Mails
Wollen Banken, Behörden oder Geschäftspartner sensible Daten wissen? Verweist eine kryptische E-Mail auf weitere Informationen im Anhang? Dann sollten Sie stutzig werden und auf keinen Fall auf die E-Mail antworten, Links folgen oder Anhänge öffnen. In Zweifelsfällen fragen Sie beim Absender nach – aber nicht per E-Mail, sondern am Telefon! Auch eine Google-Suche nach den ersten Sätzen der verdächtigen Mail kann sinnvoll sein – weil Sie so auch Warnungen vor der Betrugsmasche finden.

6. Löschen Sie lieber eine E-Mail zu viel als eine zu wenig
Erscheint Ihnen eine E-Mail als nicht glaubwürdig, löschen Sie die E-Mail aus Ihrem Postfach – und leeren Sie danach auch den Papierkorb Ihres Mailprogramms.

»Viele gehen zu sorglos mit ihren Daten um«

Mit dem Analyse-Tool cysmo findet der IT-Berater Jonas Schwade auch ohne Penetrationstests Schutzlücken in IT-Systemen.

Herr Schwade, Sie haben für den GDV die IT-Systeme von über 2.500 mittelständischen Unternehmen des produzierenden Gewerbes mit dem Analyse-Tool cysmo überprüft. Dabei sind Sie zum Teil auch auf sehr alte Systeme gestoßen – überrascht?
Jonas Schwade: Überrascht nicht – erschrocken ja. Leider setzen Unternehmen immer noch veraltete Betriebssysteme mit nicht mehr geupdateter Software ein. In dem geprüften Sample war das älteste noch im Einsatz befindliche System eine Debian Linux Version 4.0, die schon seit 2010 nicht mehr mit Updates vom Hersteller versorgt wird.

Welches Risiko besteht, wenn Unternehmen diese alten Systeme nutzen?
Schwade: In jeder Software gibt es grundsätzlich Schwachstellen, die Frage ist immer nur: „Wann werden diese entdeckt?". Im Normalfall bringen Hersteller ein Update heraus, wenn eine Sicherheitslücke bekannt wird. Solange die Updates regelmäßig eingespielt werden, sind die Systeme grundsätzlich erstmal „sicher". In dem hier vorliegenden Fall hat der Hersteller der Software vor zehn Jahren gesagt, dass diese Version zukünftig nicht mehr mit Updates versorgt wird - es hat das sogenannte end-of-life (Lebensende der Software) erreicht. Dann sollte man unbedingt auf eine neue Version umsteigen. Sonst kann es passieren, dass Wochen, Monate oder auch Jahre später eine Sicherheitslücke bekannt wird, die durch den Hersteller nicht mehr behoben wird. Für Unternehmen, die dann noch das System mit der entsprechenden Software im Einsatz haben, besteht dann die Gefahr Opfer einer Cyberattacke zu werden.

Müssen Sie für Ihre Analyse die IT-Systeme tatsächlich hacken und wenn ja: Dürfen Sie das überhaupt ohne das Wissen der Unternehmen?
Schwade: cysmo arbeitet zu 100 % passiv. Anders als bei einem Penetrationstest wird die zu analysierende Infrastruktur nicht angegriffen, sondern es werden Daten aus frei verfügbaren, offenen Quellen gesammelt und aufbereitet, im Fachjargon heißt das Open Source Intelligence (OSINT). Auf Basis dieser Daten wird eine Außensicht auf das Unternehmen erstellt und bewertet. Durch den reinen Einsatz von OSINT-Methoden bedarf es keiner Zustimmung des zu bewertenden Unternehmens und es besteht für das Unternehmen dadurch auch keine Gefahr.

Zu Ihrer Untersuchung gehört auch eine Recherche im Darknet. Wie gehen Sie bei der Suche vor?
Schwade: Tatsächlich ist das Aufspüren von Daten im Darknet deutlich schwieriger als im herkömmlichen Internet. Suchmaschinen existieren, decken aber nur einen Bruchteil der dortigen Daten ab. Auch erschweren fehlende Standards eine automatische Suche und Bewertung. cysmo prüft mit Hilfe eines Dienstleisters, ob E-Mail-Adressen oder andere technische Details des zu bewertenden Unternehmens im Darknet auftauchen.

Und obwohl die Suche also nicht ganz einfach ist, haben Sie im Darknet Daten von mehr als 1.000 der 2.500 untersuchten Firmen gefunden?
Schwade: Ja, leider ist das Auftauchen von Firmen-E-Mail-Adressen im Darknet kein Einzelfall. Die Mitarbeiter der Unternehmen gehen teils sorglos mit Ihren beruflichen E-Mail-Adressen um und melden sich damit auch in privaten Netzwerken/Diensten an. Sollte dann für den Zugang zur Musikplattform dasselbe Passwort verwendet werden wie für den Login im Mitarbeiterportal, können Angreifer diese Sorglosigkeit natürlich schnell ausnutzen.

Wie können Unternehmen verhindern, dass ihre Daten ins Darknet gelangen?
Schwade: Wir beobachten, dass unternehmensspezifische Daten primär über Datenlecks bei Drittanbietern ins Darknet gelangen und nicht direkt aus dem Unternehmensnetz entwendet werden. Da die Sicherheit der IT-Infrastruktur anderer Anbieter meist nicht in der Hand des Unternehmens liegt, hilft hier vor allem der Grundsatz der Datensparsamkeit. Mitarbeiter sollten dazu angehalten werden, umsichtig bei der Weitergabe von Daten wie E-Mail-Adressen und Telefonnummern zu sein. Im Idealfall wird die private Nutzung der geschäftlichen E-Mail-Adresse, zum Beispiel für Social Media, durch den Arbeitgeber eingeschränkt.

Achtung! Dringender Sicherheitshinweis

Kaum ein Tag vergeht ohne großangelegte Cyberattacken – dabei greifen Hacker nicht immer gezielt an, sondern suchen vor allem nach leichten Opfern. Wenn Sie nicht dazugehören wollen, sollten Sie mindestens diese drei Tipps beherzigen.

1. Schützen Sie die Zugänge zu Ihren IT-Systemen!

Ihr Passwort ist 12345? Qwertz? Passwort? Der Name Ihres Mannes? Das ist nicht gut, denn Passwörter sollen nicht leicht zu merken, sondern schwer zu knacken sein. Machen Sie es Hackern also nicht zu leicht. Am besten stellen Sie Ihre Computer-Systeme so ein, dass sie zu einfache Passwörter gar nicht erst akzeptieren oder einen zweiten Faktor zur Legitimation verlangen.

Zu einfach

Müssen Passwörter bestimmte Mindestanforderungen erfüllen?

Quelle: Forsa

15 % lassen auch einfachste Passwörter zu

Drei Tipps für sichere Passwörter

1. Denken Sie sich laaaaaaange Passwörter aus
Sonderzeichen und Großbuchstaben helfen nur bedingt weiter, ebenso das ständige Wechseln von Passwörtern. Wichtiger ist die Länge. Hacker „raten" Passwörter in der Regel nicht, sondern probieren in kurzer Zeit große Mengen möglicher Kombinationen aus. Je länger das Passwort ist, desto länger braucht auch der Computer.

2. Verwenden Sie einen Passwort-Manager
Sie und Ihre Mitarbeiter können und wollen sich die vielen langen und komplizierten Passwörter nicht merken? Dann fangen Sie auf keinen Fall an, immer das gleiche oder nur ein leicht abgewandeltes Passwort einzugeben. Das macht es Hackern zu einfach. Die bessere Alternative sind Passwort-Manager. Sie generieren und verwalten starke (=lange) Passwörter, die Sie sich nicht merken müssen; das übernimmt der Manager.

3. Nutzen Sie die Zwei-Faktor-Authentifizierung
Auch wenn es etwas komplizierter ist, sollten Sie eine Zwei-Faktor-Authentifizierung in Betracht ziehen. Dann bekommen Sie nach der Eingabe Ihres Passwortes zum Beispiel noch einen Code auf Ihr Smartphone geschickt. Alternativ bekommt jeder Mitarbeiter eine Chipkarte, mit der er sich identifizieren kann. Mit dem Passwort allein können Hacker dann nichts mehr anfangen.

2. Sichern Sie Ihre Daten richtig!

Ein Backup schützt Sie vor dem Verlust Ihrer Daten, wenn Sie keinen Zugriff mehr auf Ihre Systeme haben, etwa nach einem Brand oder einem Diebstahl. Doch dafür dürfen Sie die Kopien nicht in der Nähe der laufenden Systeme aufbewahren. Noch wichtiger: Stellen Sie durch regelmäßige Testläufe sicher, dass Ihr Backup auch wirklich funktioniert. Der Ernstfall ist der schlechteste Zeitpunkt um festzustellen, dass Ihre Sicherungskopie fehlerhaft ist.

Sichern – und dann trennen

Trennen Sie Ihre Sicherungskopien physisch vom gesicherten System?

Ja *Nein*

Quelle: Forsa

20 % bewahren ihre Backups nicht sicher auf

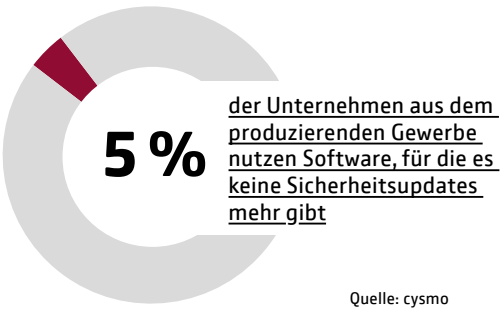
So sichern Sie Ihre Daten richtig

Was? Vom Smartphone bis zum Desktop-Rechner sollten alle Geräte gesichert werden. Kritische Daten sollten besser mehrfach gesichert werden.
Wie oft? So oft und so regelmäßig wie möglich. Stellen Sie am besten mit einem automatisierten Zeitplan sicher, dass keine Lücken entstehen.
Wohin? Speichern Sie das Backup auf jeden Fall isoliert vom Hauptsystem, also auf einer externen Festplatte, einem Netzwerkspeicher oder in einer Cloud. Kritische Daten sollten auf mindestens zwei unterschiedlichen Speichermedien liegen, von denen eines außerhalb Ihres Unternehmens liegt (z. B. in der Cloud).
Wie aufbewahren? Achten Sie darauf, dass Ihr Backup nicht mit Ihrem Hauptsystem verbunden ist – weder über Kabel noch über das WLAN.
Was noch? Testen Sie regelmäßig, ob sich die Daten Ihrer Backups im Ernstfall auch wirklich wiederherstellen lassen.

3. Halten Sie Ihren Schutz immer aktuell!

Software-Anbieter veröffentlichen für ihre Produkte regelmäßig Sicherheitsupdates. Das bedeutet auch: In der bisher benutzten Version gibt es Sicherheitslücken – und die sind Cyberkriminellen auch bekannt. Schließen Sie diese Lücken sofort und spielen Sie sämtliche Updates am besten automatisch in Ihre Systeme ein. Software, die keine Updates mehr erhält, hat auf Ihren Rechnern schon gar nichts mehr zu suchen – und dennoch sind in fünf Prozent der Unternehmen noch Programme im Einsatz, die teilweise schon seit Jahren veraltet sind.

Tickende Zeitbomben



5 % der Unternehmen aus dem produzierenden Gewerbe nutzen Software, für die es keine Sicherheitsupdates mehr gibt

Quelle: cysmo

Updates in der Warteschleife

Werden Sicherheitsupdates automatisch und zeitnah eingespielt?

Ja *Nein*

Quelle: Forsa

6 % lassen sich mit Sicherheitsupdates auch mal Zeit

Wie eine erfolgreiche Cyberattacke Unternehmen verändert

Ein erfolgreicher Cyberangriff und seine Folgen sind für viele Verantwortliche der endgültige Weckruf: Wer nicht wieder und wieder Opfer sein will, muss etwas ändern – und tut das dann auch.

Schritt 1: Eine neue Wahrnehmung

Chaos, Hilflosigkeit, hohe Kosten, Reputationsverlust – wer einmal eine Cyberattacke erlebt hat, will nie wieder in eine solche Situation kommen. Wie gravierend die Folgen eines Angriffs sein können, wird vielen Verantwortlichen erst durch die eigene Erfahrung bewusst. Bevor sie selbst betroffen sind, geht nur eine Minderheit von einem sehr hohen Risiko durch Cyberkriminalität aus. Nach einem erfolgreichen Angriff halten hingegen rund ein Drittel die Gefahr für sehr groß – und haben damit eine deutlich realistischere Einschätzung.

Schritt 2: Ein neues Handeln

Auf die Einsicht folgen in den meisten Unternehmen dann auch Taten – und die Bereitschaft, für die IT-Sicherheit Geld in die Hand zu nehmen und Strukturen zu stärken. Um künftige Angriffe besser abzuwehren und die Folgen eines erneuten Angriffs einzudämmen, sorgen die Firmen dafür, dass im Ernstfall nicht mehr plan- und kopflos, sondern schnell und konsequent reagiert wird; dafür entstehen Notfallkonzepte und entsprechende Verträge mit IT-Dienstleistern. Darüber hinaus werden Sicherheitslücken geschlossen: Egal, ob Sicherheitskopien beim ersten Angriff gefehlt haben oder funktionierende Rettungsanker in höchster Not waren – jetzt werden sie in festen Zeitabständen angefertigt und sicher aufbewahrt. Parallel verschaffen sich die Unternehmen einen besseren Überblick, wer wo wann im Netzwerk was genau macht. Dafür bekommt jeder Mitarbeiter einen persönlichen und mit einem Passwort geschützten Zugang.

Schritt 3: Ein neues (Un-)Sicherheitsgefühl

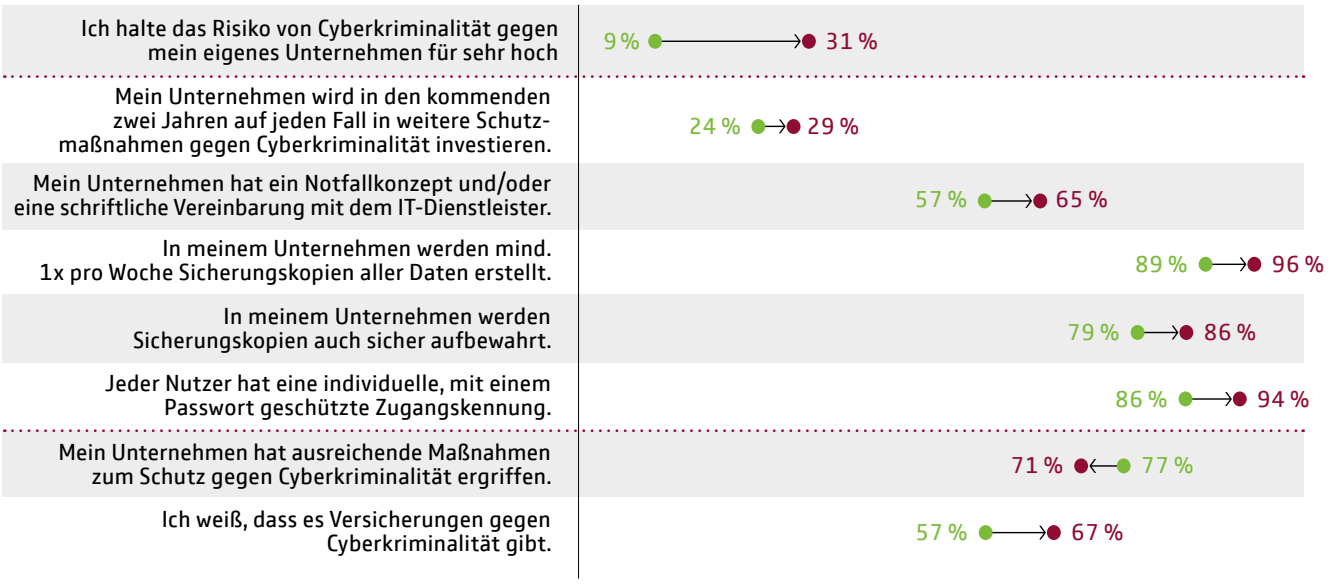
Am Ende sind die Betroffenen für einen erneuten Angriff besser gewappnet als beim ersten Mal – und wissen trotzdem, dass sie völlige Sicherheit nicht erreichen können. Obwohl sie deutlich besser vorbereitet sind als früher, bleibt ein Unsicherheitsgefühl zurück. Daher beschäftigen sich die Opfer von Cyberattacken auch häufiger mit einem möglichen Versicherungsschutz gegen Cybergefahren.

Lernen durch Schmerzen

Diese Konsequenzen ziehen Opfer aus dem produzierenden Gewerbe nach einer erfolgreichen Cyberattacke

Unternehmen ohne Schäden durch Cyberangriffe — *Unternehmen mit Schäden durch Cyberangriffe*

Quelle: Forsa



»Ransomware ist derzeit die größte Bedrohung«

Der Maschinenbau ist der größte industrielle Arbeitgeber in Deutschland, der Verband Deutscher Maschinen- und Anlagenbau e. V. (VDMA) mit rund 3.300 überwiegend mittelständischen Mitgliedern Europas größter Industrieverband. Wir sprachen mit Steffen Zimmermann, Leiter des VDMA-Competence Centers Industrial Security, über IT- und Product Security, die Chancen und Risiken durch Industrie 4.0 und Phishing-Kampagnen zur Abwehr von Ransomware.

Herr Zimmermann, Sie leiten beim VDMA das Competence Center Industrial Security, das sich um zahlreiche Facetten von Sicherheit kümmert – welchen Stellenwert hat die Sicherheit bei den Maschinenbauern?
Neben der „Safety" steht seit langem auch die Security im Fokus der Maschinen- und Anlagenbauer. Hier gibt es grundsätzlich drei Security-Bereiche: IT-Security, OT-Security und Product Security. Die IT-Security ist dabei der etablierteste Teil, denn digital vernetzt sind die Maschinenbauer nicht erst mit Industrie 4.0. IT-Sicherheit ist durchaus gelebte Praxis. Operational Technology Security und Product Security für den Maschinenpark sind deutlich jünger, und durch lange Nutzungszeiträume und Prozessabhängigkeiten auch deutlich komplexer.

Was sind Ihrer Erfahrung nach aktuell die größten Herausforderungen der VDMA-Mitgliedsunternehmen hinsichtlich ihrer Cybersicherheit?
Derzeit stellt Ransomware die größte Bedrohung dar. Gezielte Angriffe auf Weltmarktführer mit Schäden im Millionenbereich. Daneben ist die Herausforderung in der Aus- und Weiterbildung von Ingenieuren zu sehen, Security muss in die Maschinenbauprodukte integriert werden. Nicht zuletzt fehlt es an Experten und Lösungen, die Dinge auch umzusetzen.

Umfragen und Studien haben wiederholt gezeigt, dass das Niveau der IT-Sicherheit mit der Unternehmensgröße zunimmt, also gerade kleinere Unternehmen sich mit ausreichendem Schutz schwer tun. Trifft das auch auf die Maschinen- und Anlagenbauer zu?
Security kostet Geld. Die Mittel kommen auch bei uns aus dem IT-Budget und wachsen mit der Betriebsgröße. Die Herausforderung ist nicht die Technik, sondern die organisatorische Umsetzung. Der „IT-Grundschutz" muss anwendbar sein! In Unternehmen mit bis zu 250 Mitarbeitern finden Sie weniger oft einen IT-Sicherheitsexperten. Zudem gilt der Maschinenbau für IT-ler auf den ersten Blick weder als sexy noch ertragreich. Dabei gibt es gerade hier die Themen der Zukunft, deren Absicherung die Unternehmen stark zunehmend im Fokus haben.

„Security kostet Geld."

Steffen Zimmermann, Leiter des VDMA-Competence Centers Industrial Security

Bei produzierenden Unternehmen liegen Risiken nicht nur in der Office-IT, sondern auch in den Produktionsumgebungen. Ist die Gefahr von Cyberkriminalität ein Hemmschuh für die weitere Entwicklung der Industrie 4.0?
Die Chancen durch Industrie 4.0 überwiegen klar die Risiken. Doch Industrie 4.0 wird langfristig nur funktionieren, wenn Security in Entwicklung und Betrieb angemessen berücksichtigt wird. Aus meiner Sicht ist das kein Hemmschuh für Industrie 4.0, sondern ein Schub für die Security, die damit digitale Geschäftsmodelle erst ermöglicht.

Wie hilft Ihr Competence Center den VDMA-Mitgliedsunternehmen konkret?
Wir erarbeiten konkrete Praxishilfen, z. B. zu Ransomware, entwickeln Lerninhalte für IEC 62443, Security by Design und bieten in unseren Security-Arbeitskreisen eine etablierte Austauschplattform zwischen Automatisierern, Maschinenbauern, Security-Experten und dem BSI.

Immer wieder kommen Cyberangriffe nur deshalb ans Ziel, weil ein einzelner Mitarbeiter einen verseuchten Anhang öffnet oder falschen Link anklickt. Was raten Sie Unternehmen, um die Aufmerksamkeit und Vorsicht der Belegschaft nachhaltig zu steigern?
Unsere Mitglieder haben gute Erfahrungen mit Phishing-Kampagnen gemacht, z. B. mit Gophish. Besonders gefährdete Gruppen können so zielgerichtet sensibilisiert werden. Regelmäßige Informationen über aktuelle Angriffe, eine persönliche Erreichbarkeit und der klassische „Take Home Value" helfen, die Awareness hoch zu halten.

Wie gut ist Ihre IT-Sicherheit?

Absolute Sicherheit im Netz gibt es nicht. Doch Widerstand gegen Cyberkriminelle ist möglich. Wer die Gefahren realistisch einschätzt und bei seiner IT-Sicherheit die folgenden Grundlagen beachtet, ist gegen viele Angriffe wirksam geschützt und kann die wirtschaftlichen Folgen eines erfolgreichen Angriffs eindämmen. Die Forsa-Umfrage des GDV zeigt aber: An vielen Stellen klaffen Lücken in der IT-Sicherheit (Angaben in Prozent).

Der **Cyber-Sicherheits-check des GDV** unter www.gdv.de/cybercheck stellt Ihnen die wichtigsten Fragen rund um Ihre IT-Sicherheit. So finden Sie schnell heraus, wie sicher Ihre Systeme sind, wo Sie Schwachstellen haben und wie Sie diese schließen können. Ob Sie die zehn grundlegenden Anforderungen erfüllen, können Sie gleich hier beantworten. Wie gut Sie dabei abgeschnitten haben und ob es andere besser machen, können Sie auf Seite 26 herausfinden.

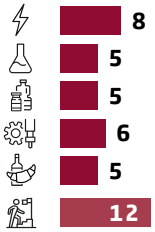
Anteil der Unternehmen, die den Schutz nicht erfüllen, nach Branche

Elektro *Chemie* *Kunststoffverarbeitung*
Maschinenbau *Lebensmittel* *Mittelstand (branchenübergr.)*

Selbsttest

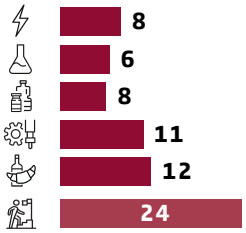
1. Sicherheitsupdates automatisch und zeitnah einspielen und alle Systeme auf dem aktuellen Stand halten

Die meiste Software erhält regelmäßig Updates. Sie dienen oft dazu, bekannt gewordene Sicherheitslücken zu schließen. Das Installieren der Updates schützt die Systeme vor Angreifern.



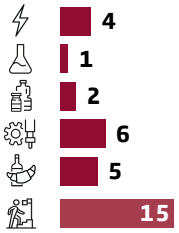
2. Mindestens einmal wöchentlich Sicherungskopien machen

Daten und digitale Systeme können gezielt angegriffen, versehentlich gelöscht oder durch Hardware zerstört werden. Deshalb ist es dringend nötig, die vorhandenen Daten regelmäßig zu sichern. Grundsätzlich gilt: Je öfter Sie Ihre Daten sichern, desto besser.



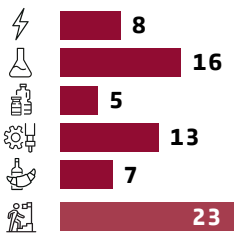
3. Administratoren-Rechte nur an Administratoren vergeben

Wer mit Administrator-Rechten an einem IT-System arbeitet, kann dabei verheerende Schäden anrichten. Deshalb ist es ratsam, solche Rechte nur sehr sparsam zu vergeben und nur dann zu nutzen, wenn sie für die aktuelle Aufgabe wirklich nötig sind.



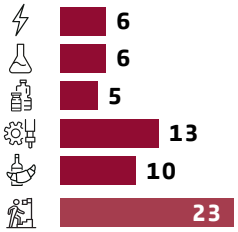
4. Alle Systeme, die über das Internet erreichbar oder im mobilen Einsatz sind, zusätzlich schützen

Mobile Geräte können leicht verloren gehen oder gestohlen werden. Sind die darauf gespeicherten Daten nicht verschlüsselt, können sie vollständig ausgelesen werden – selbst wenn sie mit einem Passwort geschützt sind. Server sind über das Internet ständig erreichbar und daher für Angriffe besonders beliebte Ziele. Sie sollten am besten mit einer 2-Faktor-Authentifizierung gesichert werden.



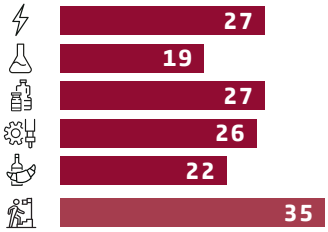
5. Manipulationen und unberechtigten Zugriff auf Sicherungskopien verhindern

Backups sind die Rückversicherung für den Fall gelöschter oder manipulierter Daten. Gesonderte Authentifizierungsstufen und ein entsprechendes Rechtemanagement sollten daher die versehentliche oder absichtliche Manipulation gesicherter Daten ausschließen.



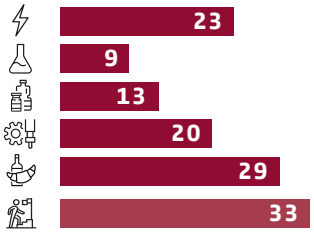
6. Alle Systeme mit einem Schutz gegen Schadsoftware ausstatten und diesen automatisch aktualisieren lassen

Viren, Trojaner oder Ransomware: Die meisten Schäden entstehen durch das unbeabsichtigte Infizieren der Systeme mit so genannter Schadsoftware. Auch wenn Virenscanner hier keinen hundertprozentigen Schutz bieten, sollte mindestens einer auf den Systemen installiert sein und regelmäßig aktualisiert werden.



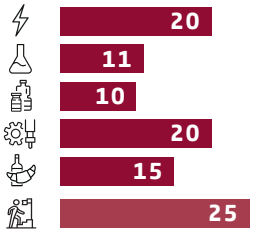
7. Sicherungskopien physisch vom gesicherten System trennen

Datensicherungen können auch dann vor dem Verlust Ihrer Daten schützen, wenn die Systeme gestohlen oder durch einen Brand zerstört wurden. Deshalb ist es ratsam, die Backups nicht in der Nähe der laufenden Systeme aufzubewahren, sondern mindestens in anderen Brandabschnitten, besser jedoch an einem ganz anderen Ort.



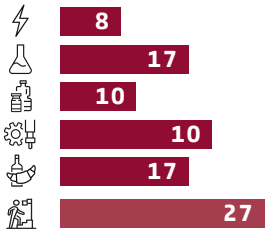
8. Mindestanforderungen für Passwörter (z.B. Länge, Sonderzeichen) verlangen und technisch erzwingen

Gerade wenn Passwörter das einzige Authentifizierungsmittel sind, sollte eine geeignete Passwortstärke technisch erzwungen werden. Andernfalls sind IT-Systeme schon durch einfachste Angriffe gefährdet.



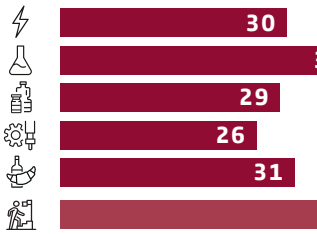
9. Jeden Nutzer mit eigener Zugangskennung und individuellem Passwort ausstatten

Ohne benutzerindividuelle Kennungen ist es nicht möglich, den Zugang zu Systemen zu sichern. Die individuelle Authentifizierung ist auch deswegen wichtig, weil nur so später nachvollzogen werden kann, wer das System wann verwendet hat.



10. Wiederherstellen der Daten aus der Sicherungskopie regelmäßig testen

Regelmäßige Testläufe stellen sicher, dass bei der Sicherungskopie keine Datenquelle fehlt und die Wiederherstellung tatsächlich funktioniert. Der Notfall ist der schlechteste Zeitpunkt um festzustellen, dass eine Sicherungskopie fehlerhaft ist.



Ergebnis: Ich erfülle _____ von 10 Maßnahmen

So gut ist Ihre IT-Sicherheit – und so gut sind die anderen

Die Schutzmaßnahmen auf den Seiten 24/25 sind nicht der Goldstandard und auch kein Garant für volle Sicherheit, sondern nur die Basis – doch schon hier haben die meisten Unternehmen Lücken. Wie viele der zehn Schutzmaßnahmen haben Sie umgesetzt?

10
Herzlichen Glückwunsch! Durch das hohe Niveau Ihrer IT-Sicherheit halten Sie das Risiko einer erfolgreichen Cyberattacke so gering wie möglich. Bleiben Sie trotzdem aufmerksam – absolute Sicherheit gibt es nicht.

8–9
Das Niveau Ihrer IT-Sicherheit ist leider noch nicht perfekt – beachten Sie unsere Hinweise und schließen sie die noch vorhandenen Sicherheitslücken.

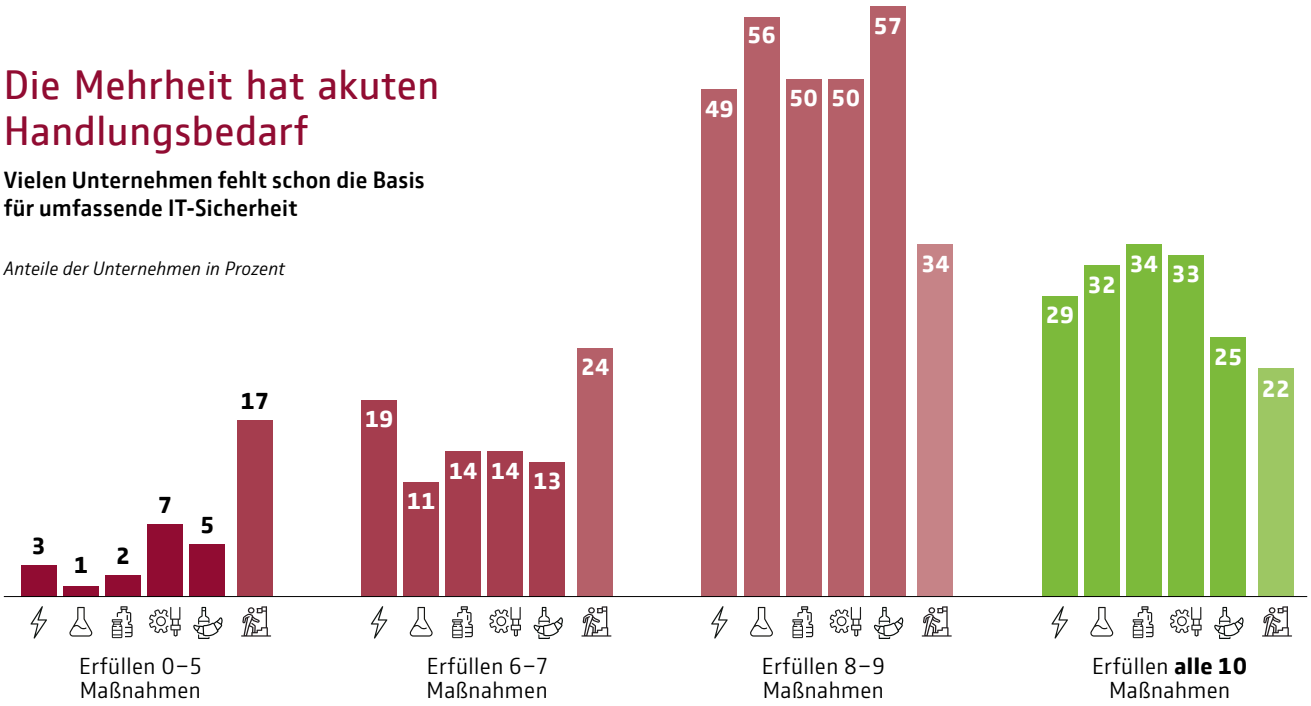
6–7
Über gute Ansätze kommt Ihre IT-Sicherheit leider nicht hinaus. Machen Sie es Cyberkriminellen nicht zu einfach und kümmern Sie sich möglichst schnell darum, Ihre Sicherheitslücken zu schließen.

0–5
Achtung, Ihre IT-Sicherheit weist deutliche Schwächen auf und kann Ihr Unternehmen zur leichten Beute für Hacker machen. Beachten Sie unsere Hinweise und holen Sie sich am besten professionelle Hilfe, um Ihren Schutz gegen Cyberrisiken schnell zu verbessern.

Die Mehrheit hat akuten Handlungsbedarf

Vielen Unternehmen fehlt schon die Basis für umfassende IT-Sicherheit

Anteile der Unternehmen in Prozent



Das leistet eine Cyberversicherung

Der Gesamtverband der Deutschen Versicherungswirtschaft hat unverbindliche Musterbedingungen für eine Cyberversicherung entwickelt. Sie sind speziell auf die Bedürfnisse von kleinen und mittleren Unternehmen zugeschnitten und richten sich sowohl an Arztpraxen oder Anwaltskanzleien als auch an Handwerksbetriebe und Industriezulieferer. Die Versicherung übernimmt nicht nur die Kosten durch Datendiebstähle, Betriebsunterbrechungen und für den Schadenersatz an Dritte, sondern steht den Kunden im Ernstfall mit einem umfangreichen Service-Angebot zur Seite: Nach einem erfolgreichen Angriff schickt und bezahlt die Versicherung Experten für IT-Forensik, vermittelt spezialisierte Anwälte und Krisenkommunikatoren. So hilft sie, den Schaden für das betroffene Unternehmen so gering wie möglich zu halten.

	Schaden	Leistung
Eigenschäden	Wirtschaftliche Schäden durch Betriebsunterbrechung.	Zahlung eines Tagessatzes.
	Kosten der Datenwiederherstellung und System-Rekonstruktion.	Übernahme der Kosten.
Drittschäden	Schadenersatzforderungen von Kunden wegen Datenmissbrauch und/oder Lieferverzug.	Entschädigung und Abwehr unberechtigter Forderungen.
Service-Leistungen	IT-Forensik-Experten zur Analyse, Beweissicherung und Schadenbegrenzung.	Jeweils Vermittlung und Kostenübernahme.
	Anwälte für IT- und Datenschutzrecht zur Beratung.	
	PR-Spezialisten für Krisenkommunikation zur Eindämmung des Imageschadens.	

Impressum

Herausgeber:
Gesamtverband der Deutschen Versicherungswirtschaft e. V.
Wilhelmstraße 43 / 43 G
10117 Berlin
Tel. +49 30 2020-5000
berlin@gdv.de, www.gdv.de

V.i.S.d.P.:
Jörn Paterak

Redaktion:
Simon Frost, Christian Siemens

Bildnachweis:
Titel: shutterstock/Pixels Hunter; S. 4/5: gettyimages/5m3photos; S. 12: shutterstock/Gorodenkoff; S. 14: shutterstock/Sergey Nivens, Uwe Klössing (M. Wiesner); S. 16: shutterstock/A. Oakenman; S. 20: shutterstock/13_Phunkod

CYBER SICHER

Eine Initiative der deutschen Versicherer.

GDV
DIE DEUTSCHEN VERSICHERER

Wilhelmstraße 43 / 43 G
10117 Berlin
Tel. +49 30 2020-5000
Fax +49 30 2020-6000
E-Mail: berlin@gdv.de

23, Rue du Champ de Mars
B-1050 Brüssel
Tel. +32 2 28247-30
Fax +32 2 28247-39
E-Mail: bruessel@gdv.de

www.gdv.de
www.DieVERSiCHERER.de
facebook.com/DieVERSiCHERER.de
Twitter: @gdv_de
www.youtube.com/user/GDVBerlin