Cyber-sicherheit

Umfrage zur Bedrohungslage

mit Empfehlungen für die Praxis

APRIL 2023

Industrie 2025

SWISSMEM

Industrie 2025 treibt die digitale Transformation auf dem Werkplatz Schweiz voran. Die Initiative unterstützt die Einführung und Verankerung von Industrie-4.0-Konzepten in Produktionsunternehmen. Dies geschieht über vielfältige Aktivitäten wie Seminare und Workshops, Arbeitsgruppen und Dienstleistungen.

:: +41 44 384 41 11
:: industrie2025.ch

Swissmem vereint über 1‘300 Unternehmen der schweizerischen Maschinen-, Elektro- und Metall-Industrie. Wir vertreten die Anliegen dieser innovativen High-Tech-Branche wirkungsvoll in der Öffentlichkeit und Politik. Als Service Center bieten wir umfassende Dienstleistungen für unsere Mitgliedsfirmen.

:: +41 44 384 41 11
:: swissmem.ch

Editorial

Philip Hauri
Geschäftsleiter
Industrie 2025

philip.hauri@industrie2025.ch
T +41 44 384 42 02

Cyberangriffe gehören heute zur Tagesordnung. Auch die Industrie ist bedroht, soviel steht fest. Doch wie ernst ist die Lage? Wir wollten es genau wissen und haben gemeinsam mit dem Institut für Strafrecht und Kriminologie der Universität Bern die Mitglieder von Swissmem befragt. Unsere Umfrage ist die erste Erhebung zur Cybersicherheit in der Schweizer Industrie.

Die Resultate bestätigen den Verdacht: Die grosse Mehrheit der Unternehmen wurde bereits attackiert – die meisten mehrmals. Überraschend ist, wie gezielt Cyberkriminelle die Industrie ins Visier nehmen. Die häufigste Angriffsart ist CEO-Fraud – eine besonders aufwändige Form von Cyberkriminalität. Die Folgen sind kostspielig: Fast ein Fünftel berichtet Schäden zwischen 100’000 Franken und einer Million. Für kleinere Unternehmen kann dies existenzbedrohend sein.

Erfreulich ist, dass MEM-Unternehmen bereits eine breite Palette von Schutzmassnahmen implementiert haben. Viele Betriebe sind für die Gefahren sensibilisiert und bauen ihre Sicherheitsmassnahmen aus. Damit Sie Ihre digitale Resilienz gezielt verbessern können, haben wir Empfehlungen von betroffenen Unternehmen und Experten gesammelt und teilen Erkenntnisse aus unseren Workshops zum Thema.

Philip Hauri

Inhalt

Einleitung

1.1 Die fünf wichtigsten Erkenntnisse

01 Mehrheit der MEM-Unternehmen ist von Cyberangriffen betroffen

80 Prozent der Unternehmen haben bereits mindestens eine der abgefragten Angriffsarten erlebt. Die meisten wurden mehrfach angegriffen. Über 10 Prozent wurden im Laufe der letzten zwei Jahre mehr als 20 Mal attackiert.

02 Der häufigste Vorfall ist CEO-Fraud

Über 54 Prozent wurden bereits Opfer eines CEO-Fraud. Dabei versuchen Kriminelle unter Verwendung einer falschen Identität Geldüberweisungen zu erwirken. Das ist überraschend, weil dies eine gezielte und besonders aufwändige Angriffsart ist.

03 Gezielte Angriffe zielen meist auf Erpressung ab

Mehr als ein Fünftel der betroffenen Unternehmen geht davon aus, dass sie gezielt attackiert wurden. Als Grund dafür wird meist das hohe Ertragspotenzial genannt. Rund 5 Prozent der befragten Unternehmen waren bereits einmal Opfer einer Erpressung.

04 Folgekosten können existenzbedrohend sein

Bei fast einem Fünftel der befragten Unternehmen verursachten die Angriffe Kosten zwischen 100’000 Franken und einer Million. In fünf Fällen war der Schaden noch höher. Bei zwei Firmen gefährdete der Angriff gar die Existenz des Unternehmens.

05 Schutzmassnahmen sind auf breiter Ebene etabliert

Im Durchschnitt verfügen die Unternehmen über rund 25 von 34 abgefragten Schutz- und Interventionsmassnahmen. Fast alle setzen die technischen Basics um. Über drei Viertel verfügen zudem über Notfallpläne und führen regelmässig Schulungen durch.

1.2 Interview mit Martin Hirzel Swissmem

Martin Hirzel

Ist seit über 20 Jahren in der Schweizer Industrie tätig. Bis Ende 2019 war er während neun Jahren CEO der Autoneum Holding AG. Davor führte er vier Jahre lang die Marktregion Südamerika, Mittlerer Osten & Afrika und zwischen 2000 und 2007 verantwortete er in Shanghai den Aufbau der lokalen Präsenz der Rieter Holding AG. Martin Hirzel ist seit Januar 2021 Swissmem-Präsident und Mitglied des Verwaltungsrats der Bucher Industries AG und der Dätwyler Holding AG.

Swissmem-Präsident Martin Hirzel über die akute Bedrohungslage, die teuren Folgen und den wachsenden Zielkonflikt zwischen Abwehrmassnahmen und Digitalisierung.

Welches Fazit ziehen Sie aus der Befragung?

Martin Hirzel: Industriefirmen müssen jederzeit mit Angriffen rechnen. Es kann jedes Unternehmen unabhängig von seiner Grösse treffen und das Schadenspotenzial ist enorm. Jeder Betrieb muss technologisch und organisatorisch stets vorbereitet sein, um solche Attacken abwehren zu können. Das gehört genauso zum betrieblichen Alltag, wie Rechnungen bezahlen.

Was sind die Folgen, wenn nicht genügend für die Sicherheit getan wird?

Bei jedem sechsten Unternehmen führte der Angriff zu spürbaren betrieblichen Einschränkungen. Cyberattacken haben schwerwiegende und kostspielige Folgen. In fast einem Fünftel der befragten Unternehmen verursachten die Angriffe einen Schaden zwischen 100’000 Franken und einer Million. Für kleinere Unternehmen kann das existenzbedrohend sein.

> «Das Schadenspotenzial ist enorm.»

Was macht die Vorfälle so kostspielig?

Ins Geld gehen vor allem Sofortmassnahmen zur Abwehr und Aufklärung, für externe Beratung, für Investitionen in Sicherheitsmassnahmen sowie für spezifische Versicherungen. Aber auch Betriebsunterbrechungen und die Wiederherstellung von Daten oder der IT-Infrastruktur sind kostenintensiv.

Wo lauern die grössten Risiken?

CEO-Fraud ist die häufigste Angriffsart. Das ist überraschend, weil es sich dabei um sehr aufwändige, gezielte Attacken handelt. Dabei versuchen Kriminelle unter Verwendung einer falschen Identität Geldüberweisungen zu erwirken. Sehr verbreitet sind zudem Phishing-Attacken. Ziel dieser Angriffe ist es, Zugang zu den ICT-Systemen zu erhalten, um illegal an wertvolle Daten zu gelangen.

Sind sich die Unternehmen der Bedrohungslage bewusst?

Es ist erfreulich, dass in unserer Branche eine hohe Sensibilisierung in Bezug Cyberrisiken besteht. In fast allen Betrieben ist Sicherheit ein Thema und es ist klar zu erkennen, dass die Firmen nach Angriffen in systematische Massnahmen – wie zum Beispiel Risikoanalysen oder Monitoring der ICT-Aktivitäten – investiert haben. Das gilt für Grossfirmen und KMU. Im Durchschnitt haben die Swissmem-Mitglieder über 25 Schutz- und Interventionsmassnahmen im Einsatz. Die Aufmerksamkeit darf jedoch niemals nachlassen. Sicherheit ist ein dynamischer Prozess – und Sicherheit ist Chefsache.

> «Cyberattacken können für kleinere Unternehmen existenzbedrohend sein.»

Wo liegen die grössten Herausforderungen bei der Prävention?

Viele Industrieunternehmen sehen sich angesichts der Bedrohungslage in einem Zielkonflikt. Einerseits sind sie gefordert, in die Digitalisierung der betrieblichen Prozesse, Produkte und Dienstleistungen zu investieren. Das erfordert eine immer intensivere, teils unternehmensübergreifende Vernetzung der Systeme. Andererseits erfordert der Schutz eben dieser Systeme, bei der Vernetzung vorsichtig vorzugehen.

Wie unterstützt Swissmem ihre Verbandsmitglieder bei dieser Gratwanderung?

Die Initiative «Industrie 2025» wird von den Verbänden Swissmem, asut und swissT.net getragen und hat sich zum Ziel gesetzt, die digitale Transformation auf dem Werkplatz Schweiz voranzutreiben. Unter der Bezeichnung «Security 2025» wurde ein spezielles Angebot für Industriebetriebe geschaffen. Dabei helfen Experten insbesondere KMU, die Sicherheitsthemen anwendungs- und praxisbezogen anzugehen.

1.3 Über die Umfrage

Swissmem und die Initiative «Industrie 2025» haben das Institut für Strafrecht und Kriminologie der Universität Bern beauftragt, eine Online-Befragung zum Thema Cybersicherheit in der Maschinen-, Elektro- und Metall-Industrie durchzuführen. Die Ergebnisse wurden am Swissmem-Industrietag vom 23. Juni 2022 präsentiert. Die vorliegende Publikation fasst die wichtigsten Erkenntnisse zusammen. Den vollständigen Studienbericht finden Sie unter folgendem Link:

www.boris.unibe.ch/172496

Kontakt für Fragen und weitere Informationen:

PD Dr. Ueli Hostettler, Head of the Prison Research Group Universität Bern – Institut für Strafrecht und Kriminologie Schanzeneckstrasse 1, Postfach, 3001 Bern

+41 31 684 55 83 | +41 79 751 46 92
ueli.hostettler@krim.unibe.ch
prisonresearch.ch

Durchführung und Aufbau der Umfrage

Swissmem liess die Online-Befragung zwischen dem 9. März und dem 21. April 2022 vollständig anonym durchführen. Der Fragebogen wurde an 1'300 Mitgliedsfirmen versandt. Insgesamt 271 Unternehmen haben den Fragebogen so weit ausgefüllt, dass ihre Antworten in die Analyse einbezogen werden konnten. Das entspricht einem Rücklauf von rund 23 Prozent.

Die Umfrageteilnehmer wurden zunächst befragt, inwiefern sie in der Vergangenheit durch digitale und physische Angriffe betroffen waren. Dabei wurden die Angriffe seit Gründung des Unternehmens abgefragt sowie auch die Attacken in den zwei Jahren vor der Befragung. Zum schwerwiegendsten Angriff wurden Anschlussfragen gestellt, zum Beispiel nach den betrieblichen Folgen, der Höhe des finanziellen Schadens und den betroffenen Daten. Zudem wurden auch die vorhandenen Schutz- und Interventionsmassnahmen abgefragt.

Die einzelnen Fragen wurden von unterschiedlich vielen Unternehmen beantwortet. Dies, weil je nach Antworten gewisse Folgefragen nicht angezeigt wurden, zum Beispiel, wenn ein Unternehmen keinen schwerwiegenden Angriff vermeldete. Die Summe der Antworten wird in den Grafiken jeweils angegeben (N=Anzahl Unternehmen). Die Prozentangaben in den Darstellungen können rundungsbedingt in der Summe mehr oder auch weniger als 100 Prozent betragen.

Forschungsstand und methodische Grundlagen

Die Cybersicherheit in Schweizer Industrieunternehmen wurde bisher noch nicht spezifisch untersucht. Auch branchenübergreifend gibt es in der Schweiz erst vereinzelt Erhebungen, darunter einer Befragung von KMU zum Thema Homeoffice und Cybersicherheit, die 2020 nach Ausbruch der Coronapandemie von gfs, digitalswitzerland und Mobiliar durchgeführt wurde.

Die methodischen Grundlagen für die vorliegende Umfrage lieferten verschiedenste internationale Studien zur Cybersicherheit in Wirtschaft und Industrie. Als Inspirationsquelle diente insbesondere eine 2020 durch das Kriminologische Forschungsinstitut Niedersachsen durchgeführte Umfrage unter deutschen Unternehmen[1].

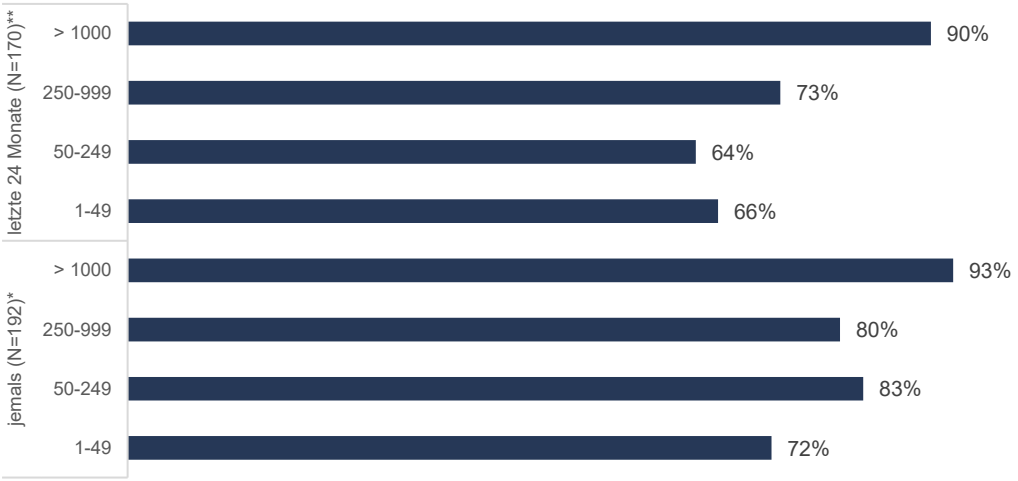
1 Cyberangriffe gegen Unternehmen - Ergebnisse einer repräsentativen Unternehmensbefragung 2018/2019 – Kurzbericht (kfn.de)

Ergebnisse der Umfrage

2.1 Bedrohungslage und Betroffenheit

Die grosse Mehrheit der befragten Swissmem-Mitglieder hat bereits mindestens eine der abgefragten Angriffsarten erlebt: 80 Prozent waren seit der Unternehmensgründung von mindestens einer Attacke betroffen. In den zwei Jahren vor der Befragung wurden rund 70 Prozent mindestens einmal angegriffen. Einige verzeichneten seit Anfang 2020 über 20 Angriffe vergleichbarer Art.

Bei den meisten Angriffsarten äusserten die Befragten für die letzten zwei Jahre vor der Befragung eine vergleichbar hohe Betroffenheit wie seit Gründung des Unternehmens. Da unter den Befragten viele Traditionsunternehmen sind, die seit Jahrzehnten existieren, muss davon ausgegangen werden, dass die Häufigkeit der Angriffe in den letzten Jahren stark zugenommen hat.



*Grafik 1: Betroffenheit seit Bestehen des Unternehmens und in den letzten 24 Monaten vor der Befragung nach Unternehmensgrösse (dargestellt sind die Anteile Betroffener; in Prozent; Chi-Quadrat Test: *p<.05, **p<.03, ***p<.001)*

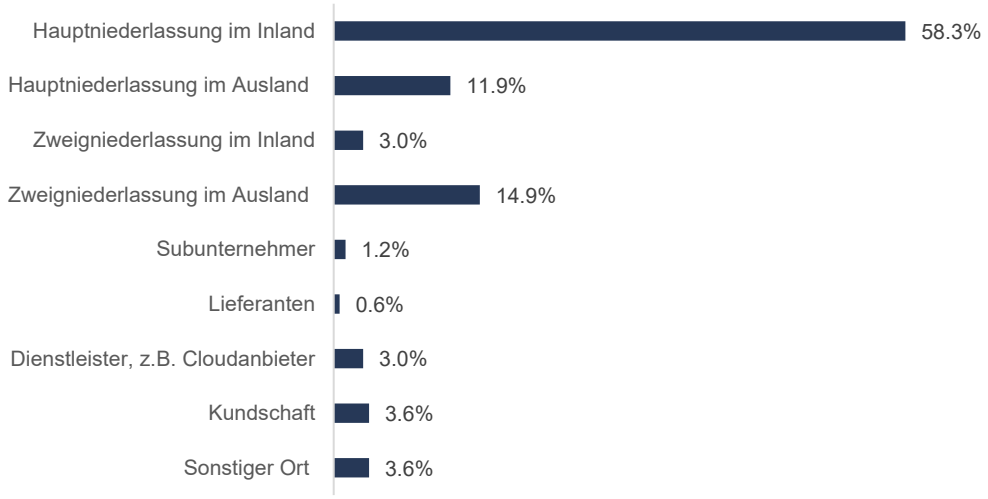
Grossunternehmen sind exponierter

Grössere Industrieunternehmen sind durch ihre globale Präsenz mit Niederlassungen rund um die Welt grundsätzlich exponierter als kleinere Produktionsbetriebe. Gleichzeitig sind sie auch finanziell attraktivere Ziele für Cyberkriminelle. Bei den Unternehmen mit über 1'000 Mitarbeitenden ist die Betroffenheit seit der Unternehmensgründung mit über 90 Prozent denn auch am grössten.

Kleinere Unternehmen sind in der Tendenz etwas weniger bedroht. Unter den 20 Prozent der Unternehmen, die bisher noch nie angegriffen worden sind, befinden sich vor allem Betriebe mit einer Grösse von 1-49 Mitarbeitenden. Auch mit Blick auf die Verbreitung der einzelnen Angriffsarten ist die Betroffenheit von der Unternehmensgrösse abhängig. Bei den Folgen zeigt sich ebenfalls eine Korrelation zwischen der Grösse der Unternehmen und dem entstandenen Schaden.

Auch Zweigniederlassungen im Ausland sind bedroht

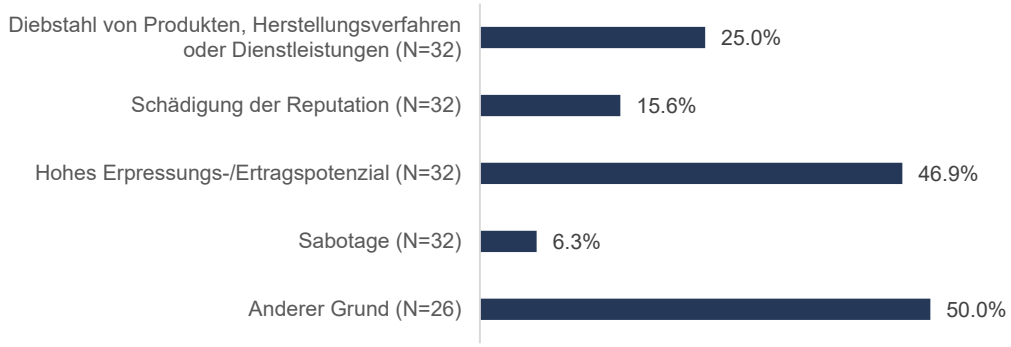
Zum schwerwiegendsten Angriff der letzten zwei Jahre wurden Vertiefungsfragen zum Ereignis gestellt. Bei den meisten Unternehmen wurde dabei zuerst die Hauptniederlassung im Inland attackiert. Grössere Unternehmen sehen jedoch auch ihre Niederlassungen im Ausland bedroht: Bei den Firmen mit mehr als 1'000 Mitarbeitenden war der initiale Angriffspunkt des schwerwiegendsten Angriffs am häufigsten eine Zweigniederlassung im Ausland. Dabei wurden am häufigsten Standorte in Deutschland, USA, Indien, China, England und Italien genannt.



Grafik 2: Initialer Angriffspunkt des schwerwiegendsten Angriffs (in Prozent; N=168)

Gezielte Angriffe zielen meist auf Erpressung ab

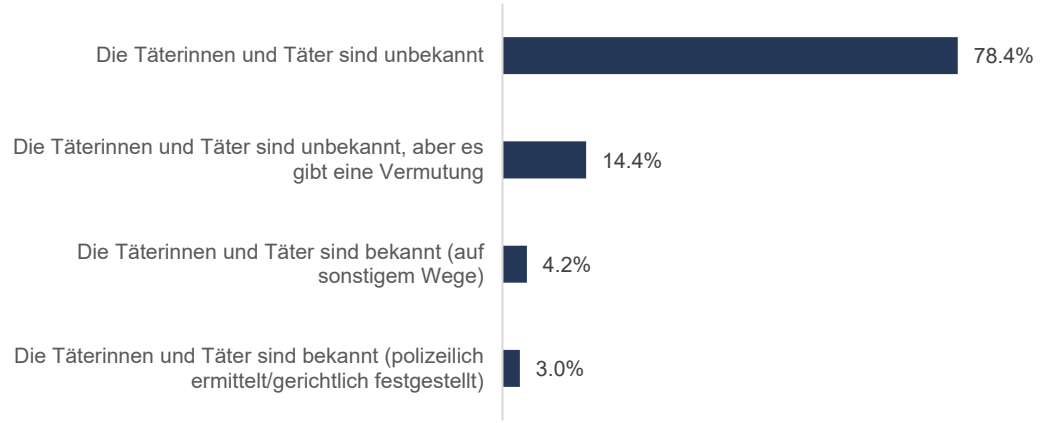
Die Mehrheit der Firmen, die Angaben zum aus ihrer Sicht schwerwiegendsten Angriff gemacht haben, vermutet, dass der Angriff mehr oder weniger zufällig im Rahmen einer Attacke auf verschiedenste Unternehmen erfolgte. Etwas mehr als ein Fünftel der Firmen geht hingegen von einer gezielten Attacke aus. Als Grund dafür nennt fast die Hälfte das hohe Erpressungs- und Ertragspotenzial. Ein Viertel sieht den gezielten Diebstahl von Produkten, Dienstleistungen, Herstellungsverfahren und Know-how als Hauptmotiv.



Grafik 3: Gründe für Zielgerichtetheit des Angriffs (Anteile: ja)

Täter werden kaum je gefasst

Die Täterschaft hinter Cyberattacken ist divers: Neben Hackern und Cyberkriminellen sind die Täter nicht selten auch aktuelle oder ehemalige Mitarbeitende. In der überwiegenden Mehrheit der Fälle blieben die Täterinnen und Täter des schwerwiegendsten Angriffs unbekannt. Jedes siebte Unternehmen hat immerhin eine Vermutung zur Täterschaft. Nur in einem Dutzend der angegebenen Fälle konnten die Täter gefasst werden.



Grafik 4: Kenntnis der Täter bzw. Täterinnen (in Prozent; N=167)

2.2 Verbreitung der Angriffsarten

Die Unternehmen wurden zu den Methoden befragt, mit denen die bisher erlebten Angriffe ausgeführt wurden. Dabei standen insgesamt 16 Angriffsarten zur Auswahl. Die Beschreibungen der Methoden stützen sich auf vergleichbare Studien. Einige Definitionen wurden von den Wissenschaftlerinnen und Wissenschaftlern der Uni Bern in Zusammenarbeit mit der Swissmem-Projektgruppe branchenspezifisch angepasst.

Die grössten Bedrohungen für die Sicherheit in der MEM-Industrie sind offensichtlich digitaler Art. Die unterschiedlichen Arten von Cyberangriffen und digitaler Datendiebstahl treten deutlich häufiger auf als physische Angriffe wie Einbrüche oder der Diebstahl von physischen Dokumenten. Klar an der Spitze stehen dabei Angriffe durch CEO-Fraud und Phishing. Auch Schadsoftware, manuelle Hackerangriffe, Ransomware, Social Engineering und (D)Dos-Attacken wurden häufig genannt. Relativ klein hingegen ist die Bedrohung durch Sabotage – sei es digital oder physisch.

Übersicht: Methoden von Cyberkriminalität

» Hackerangriff

Als Hackerangriff werden Aktivitäten bezeichnet, welche die Manipulation von Computern, Smartphones, Tablets oder ganzer Netzwerke zum Ziel haben. Diese allgemeine Bedeutung lässt sich auf manuelles Hacking eingrenzen – die Manipulation von Hard- und Software ohne die Nutzung spezieller Schadsoftware. Dabei haben Hacker nicht zwingend kriminelle Absichten. Häufig geht es ihnen auch nur darum, Schwachstellen in IT-Systemen aufzudecken.

» Phishing

Als Phishing werden Versuche bezeichnet, sich über gefälschte Webseiten, E-Mails oder Kurznachrichten als vertrauenswürdiger Kommunikationspartner auszugeben. Ziel ist es, an Daten des Internet-Nutzers zu gelangen oder ihn zur Ausführung einer bestimmten Aktion zu bewegen. In der Folge wird zum Beispiel eine Schadsoftware installiert oder es werden Finanzmittel gestohlen.

» Social Engineering

Social Engineering nennt man zwischenmenschliche Beeinflussungen mit dem Ziel, Personen zum Beispiel zur Preisgabe von vertraulichen Informationen oder zur Freigabe von Finanzmitteln zu bewegen. Dabei kommen oftmals Phising-Methoden zum Einsatz.

» CEO-Fraud

CEO-Fraud ist eine der häufigsten Formen von Social Engineering in der gegen Unternehmen gerichteten Cyberkriminalität. Meist werden im Namen des CEO E-Mails verfasst, in denen Mitarbeitenden gebeten werden, eine Zahlung zu veranlassen.

» Schadsoftware

Schadsoftware (engl. Malware) bezeichnet Programme wie Viren, Trojaner und Würmer, die schädliche Funktionen ausführen – sei es das Löschen oder Übermitteln von Dateien oder die Kompromittierung der Sicherheitssoftware. Die Schadfunktionen sind gewöhnlich getarnt oder die Software läuft unbemerkt im Hintergrund ab.

» Ransomware

Ransomware ist eine Form von Schadsoftware, die auf Lösegeldforderungen abzielt. Dabei werden Daten verschlüsselt oder Zugänge gesperrt. Die Betroffenen werden darauf zu einer Lösegeldzahlung aufgefordert, um wieder Zugriff auf die Dateien zu erhalten.

» (D)DoS-Attacke

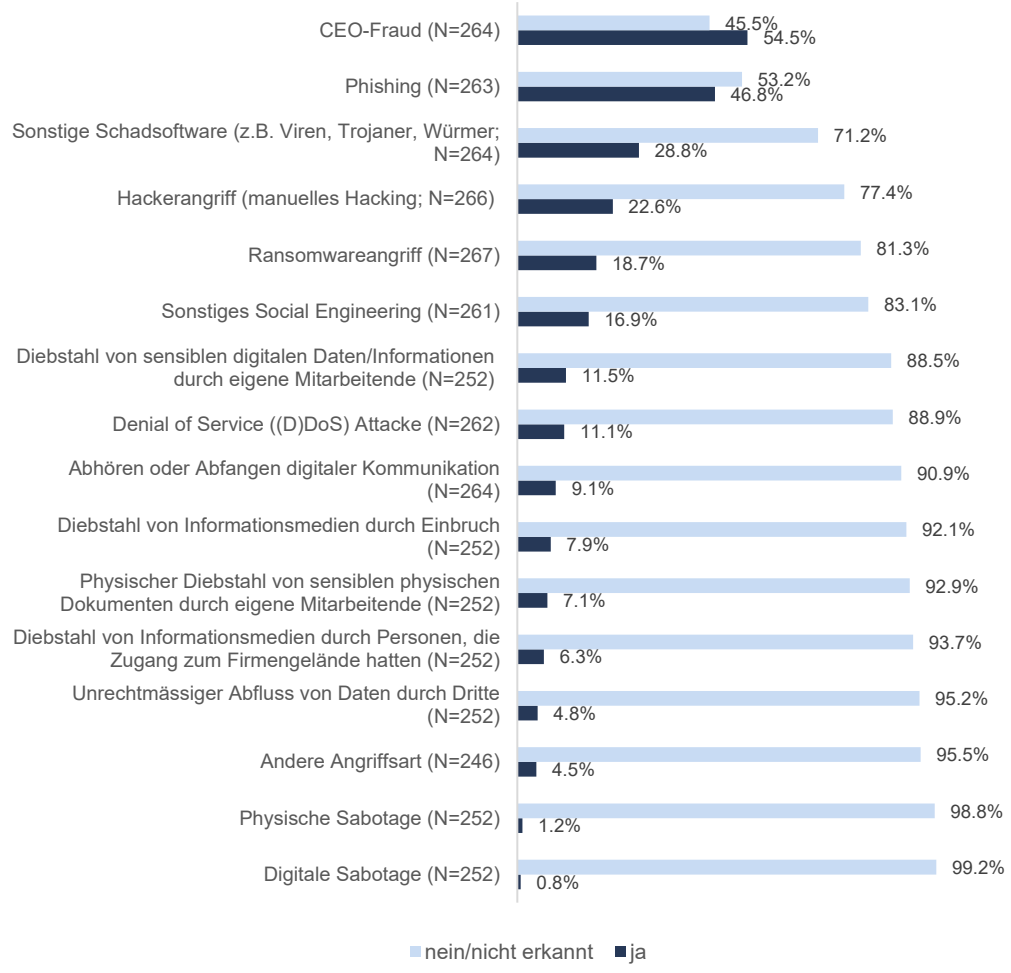
Eine DoS-Attacke hat eine Überlastung der IT-Infrastruktur zum Ziel. Das Kürzel DoS steht für «Denial of Service», auf Deutsch «Verweigerung des Dienstes». Dabei wird eine Website oder ein E-Mail-Server mit so vielen Anfragen bombardiert, dass das System seine Dienste wegen Überlastung nicht mehr erbringen kann. Bei einem Distributed Denial-of Service (DDoS) werden die Angriffe auf mehrere Systeme verteilt.

CEO-Fraud ist die häufigste Angriffsart

Eine besonders beliebte Strategie von Cyberkriminellen ist CEO-Fraud. Dabei versuchen diese unter Verwendung einer falschen Identität Geldüberweisungen zu erwirken, in der Regel mit gefälschten E-Mails im Namen von Geschäftsleitungsmitgliedern. Über 54 Prozent der befragten Unternehmen haben seit ihrer Gründung bereits einen solchen Angriff erlebt.

Damit ist CEO-Fraud die mit Abstand am meisten genannte Angriffsart – und dies ist überraschend. Zum einen, weil es sich dabei in der Regel um eine gezielte und deshalb besonders aufwändige Angriffsart handelt. Zum anderen, weil die Betroffenheit unter den Befragten deutlich grösser ist als in vergleichbaren Studien. So zeigt die ähnlich aufgebaute Erhebung des Kriminologischen Forschungsinstituts Niedersachsen eine deutlich geringere Häufigkeit dieser Methode[1].

Oft bleibt es nicht bei einem Vorfall: Rund jedes zehnte Unternehmen war in den vergangenen zwei Jahren drei- bis fünfmal von CEO-Fraud betroffen. Die Methode wird häufig mit anderen Angriffsarten kombiniert. Am verbreitetsten ist die Kombination mit Phishing und Schadsoftware – zwei Methoden, die isoliert betrachtet auf Platz 2 und 3 der meistgenannten Angriffsarten liegen.



Grafik 5: Betroffenheit durch einzelne Angriffsarten seit Bestehen des Unternehmens (sortiert nach Häufigkeit; in Prozent)

1 Cyberangriffe gegen Unternehmen - Ergebnisse einer repräsentativen Unternehmensbefragung 2018/2019 - Kurzbericht (kfn.de)

Phishing-Attacken haben die höchste Kadenz

Phishing ist die am zweithäufigsten genannte Angriffsart. Rund 47 Prozent der Unternehmen haben bereits mindestens eine solche Attacke erlebt. Ziel solcher Angriffe ist es, an sensible Daten zu gelangen. Dabei werden Mitarbeitende zum Beispiel mit gefälschten E-Mails oder Websites getäuscht, worauf sich die Täter Zugang zum IT-System verschaffen.

Auffällig ist die hohe Kadenz der Phishing-Angriffe: Über 13 Prozent der Unternehmen waren in den letzten zwei Jahren mehr als 20-mal von einem solchen Angriff betroffen. Zum Vergleich: Bei allen anderen Angriffsarten liegt dieser Wert im tiefen einstelligen Bereich oder darunter.

Die Bedrohung durch Ransomware wächst

An dritter Stelle der häufigsten Angriffsarten steht Schadsoftware. Rund 29 Prozent der Unternehmen wurde mindestens einmal von Viren, Würmern oder Trojanern angegriffen. Solche Attacken wiederholen sich jedoch eher selten und die Folgen sind meist relativ gering.

Eine der bedrohlichsten Formen von Schadsoftware ist Ransomware. Diese Angriffsart wurde in der Befragung als separate Kategorie erfasst, weil sie zielgerichteter als herkömmliche Malware. Dabei werden Daten verschlüsselt und Lösegeldforderungen gestellt. Diese Methode zählt zu den verbreitetsten Formen von Cyberkriminalität. Rund jedes fünfte Unternehmen wurde bereits Opfer eines solchen Angriffs.

Die akute Bedrohungslage spiegelt sich in den zahlreichen Medienberichten über betroffene Unternehmen, darunter immer wieder Industriebetriebe. Ransomware verbreitet sich gegenwärtig rasant. In den letzten Jahren ist eine regelrechte Industrie entstanden, die entsprechende Software an Cyberkriminelle vertreibt.

Zu den häufigsten Angriffsarten zählen zudem auch manuelle Hackerangriffe (23 Prozent), bei denen Hard- oder Software manipuliert wird. Etwas weniger häufig sind (D)Dos-Attacken (11 Prozent). Beide Methoden kommen vor allem in grösseren Unternehmen vor.

Mitarbeitende werden ausspioniert, sind oft aber auch Täter

Eine weit verbreitete Methode ist auch Social Engineering (17 Prozent). Darunter fallen Methoden, mit denen Mitarbeitende gezielt ausspioniert werden, um an vertrauliche Informationen zu kommen – sei es am Telefon, in sozialen Netzwerken oder Internetforen, im privaten Umfeld, auf Messen oder sonstigen Veranstaltungen. Bei den schwerwiegendsten Angriffen ist Social Engineering die am zweithäufigsten genannte Kategorie. Das verdeutlicht das Schadenspotenzial dieser Methode.

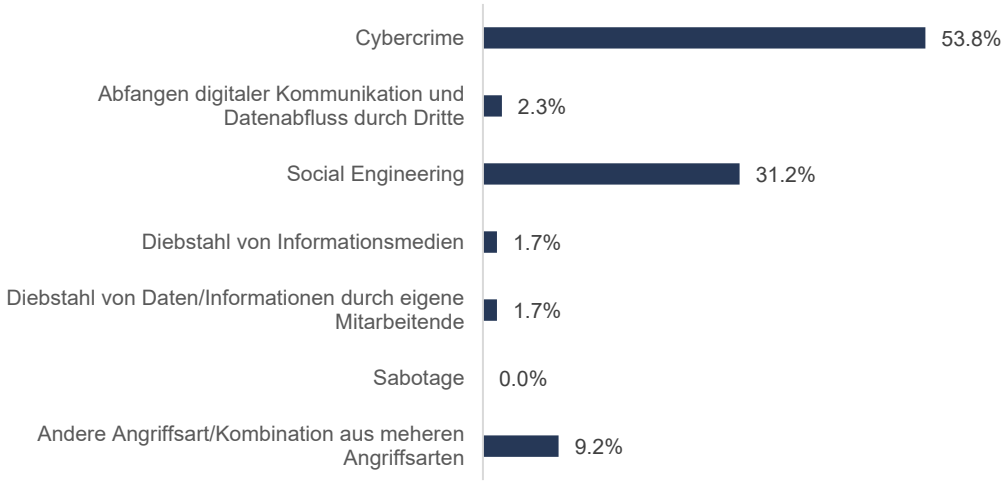
Nicht selten stammen die Täter aber auch aus der eigenen Belegschaft: Unter den abgefragten Arten des Datendiebstahls steht der Datenklau durch eigene Mitarbeitende an erster Stelle (12 Prozent), deutlich vor dem Diebstahl von Informationsmedien durch Einbruch (8 Prozent) oder dem unrechtmässigen Abfluss von sensiblen Daten durch Dritte (5 Prozent). Auch physische Dokumente werden immer wieder von eigenen Mitarbeitende entwendet (7 Prozent).

Die schwerwiegendsten Angriffe stammen meist aus dem Bereich Cyberkriminalität

Die von den befragten Unternehmen genannten schwerwiegendsten Angriffe wurden in eine der folgenden sechs Kategorien eingeteilt: Cyberkriminalität, Abfangen digitaler Kommunikation oder Daten durch Dritte, Social Engineering, Diebstahl von Informationsmedien durch Dritte bzw. durch eigene Mitarbeitende sowie Sabotage. Zudem wurde ein Sammelgefäss für weitere Angriffsarten und die Kombination von mehreren Methoden gebildet.

Mehr als die Hälfte der schwerwiegendsten Angriffe stammen aus dem Bereich Cyberkriminalität. Darunter fällt eine Reihe von Methoden wie Phishing oder Ransomware. An zweiter Stelle steht mit einem Anteil von knapp zwei Dritteln Social Engineering. Dazu zählen neben CEO-Fraud – der wie bereits erwähnt meistgenannten Angriffsform – auch sonstige Formen von Social Engineering, bei denen Mitarbeitende gezielt ausspioniert werden.

Kombinationen von mehreren Angriffsarten sowie weitere Angriffsarten machen die drittgrösste Gruppe aus. Das unterstreicht: Die Ausprägungen von Cyberangriffen sind mannigfaltig und oft werden unterschiedliche Methoden miteinander kombiniert.



Grafik 6: Art des schwerwiegendsten Angriffs (in Prozent; N=173)

Datendiebstahl und Spionage spielen eine untergeordnete Rolle

Relativ gering hingegen ist die Bedrohung durch Industriespionage und Sabotage. Nur bei den wenigsten der schwerwiegendsten Angriffe wurden Daten oder physische Medien durch Dritte gestohlen. Auch Sabotageakte wurden kaum verzeichnet.

Was ist Cyberkriminalität?

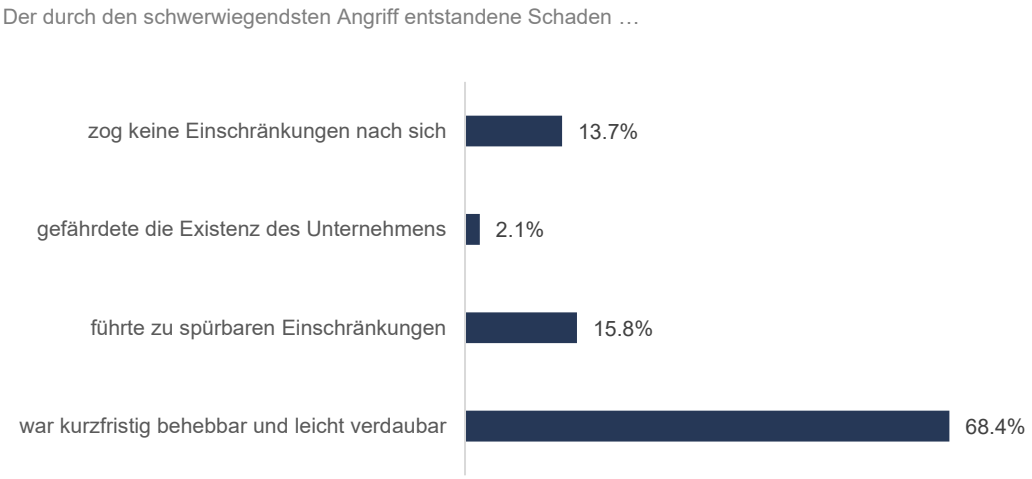
Der Begriff Cyberkriminalität bezeichnet verschiedenste Straftaten, die unter Ausnutzung der digitalen Informations- und Kommunikationstechnik begangen werden. Im Gegensatz zu nicht kriminell motivierten Hackern begehen Cyberkriminelle ganz bewusst illegale Handlungen. Dabei werden häufig verschiedene Methoden kombiniert. In der vorliegenden Umfrage wurden unter Cyberkriminalität folgende Angriffsarten subsumiert:

- Phishing-Angriffe, bei denen sich Cyberkriminelle Zugang zu sensiblen Daten verschaffen
- Hackerangriffe auf IT-Systeme und Firmengeräte, d.h. die Manipulation von Hard- und Software ohne die Nutzung spezieller Schadsoftware
- Angriffe mit Ransomware, bei denen Unternehmensdaten verschlüsselt wurden
- Angriffe mit sonstiger Schadsoftware, z.B. Viren, Würmer, Trojaner
- (D)DoS-Attacken, die auf eine Überlastung von Web- oder E-Mail-Servern zielen

2.3 Betriebliche und finanzielle Folgen

Zum schwerwiegendsten Angriff wurden vertiefende Fragen zu den Folgen für den Betrieb gestellt. Viele der betroffenen Unternehmen sind mit einem blauen Auge davongekommen: Etwas mehr als zwei Drittel gaben an, dass der Schaden kurzfristig behebbar und leicht verdaubar war. Den vielen glimpflich verlaufenen Fällen stehen einige mit schwerwiegenden Konsequenzen gegenüber. Bei 16 Prozent der Unternehmen führte der entstandene Schaden zu spürbaren Einschränkungen.

Dabei sind es meist Angriffe aus dem Bereich Cyberkriminalität, die zu betrieblichen Einschränkungen führen. Für kleinere Unternehmen können solche Attacken gar existenzbedrohend sein: In zwei Fällen gefährdete der schwerwiegendste Angriff die Existenz, wobei es sich bei beiden Firmen um Unternehmen mit weniger als 249 Mitarbeitende handelt.



Grafik 7: Nähere Angaben zum entstandenen Schaden (in Prozent; N=95)

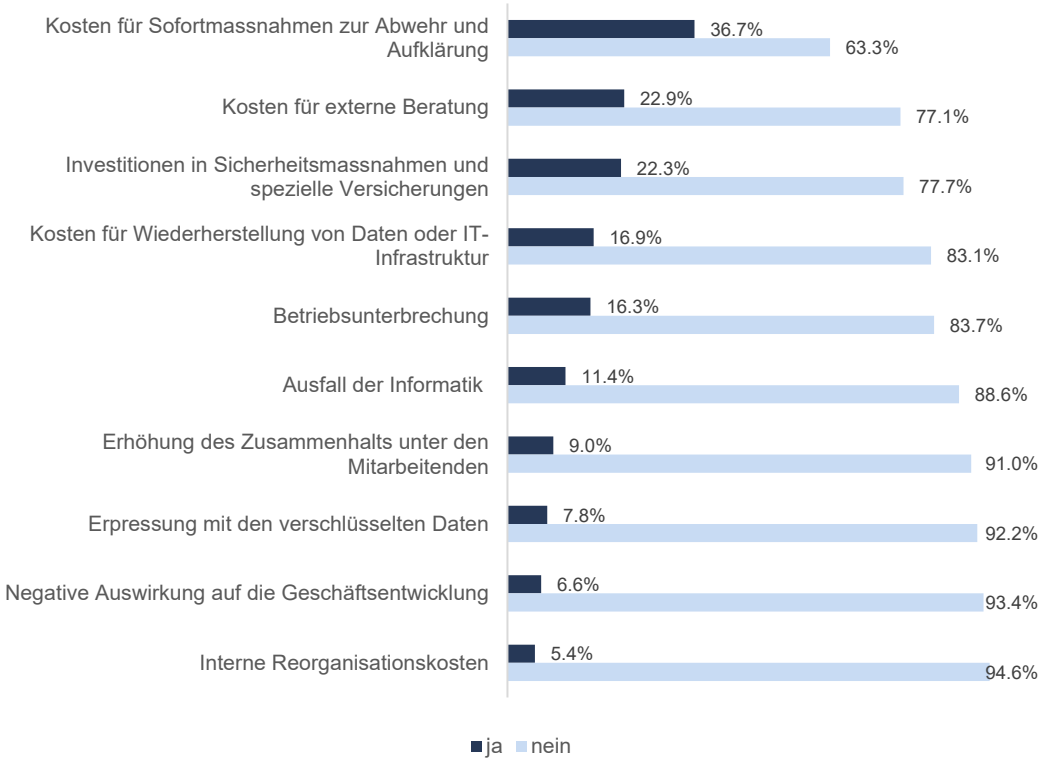
Mit Blick auf die Folgen des schwerwiegendsten Angriffs nennen die meisten Unternehmen an erster Stelle die Kosten. Ins Geld gehen in erster Linie Sofortmassnahmen zur Abwehr und Aufklärung. Rund jedes dritte Unternehmen gab dies als Folge an. Etwa ein Viertel berichtete von Kosten für externe Beratung und Investitionen in Sicherheitsmassnahmen oder spezielle Versicherungen.

Die Wiederherstellung von Daten verursacht ebenfalls häufig Kosten. Dabei sind es insbesondere personenbezogene Daten, darunter häufig auch Kundendaten, die manipuliert, verschlüsselt oder gelöscht werden. Prozess- und Produktdaten sowie auch betriebswirtschaftliche Daten müssen hingegen seltener wiederhergestellt werden.

Betriebsunterbrechungen sind häufiger als IT-Ausfälle

Cyberangriffe haben oftmals Auswirkungen auf das Tagesgeschäft: Bei etwa jedem sechsten Unternehmen führte der schwerwiegendste Angriff zu spürbaren betrieblichen Einschränkungen. Einen kompletten Ausfall der Informatik berichtete hingegen nur jedes neunte Unternehmen. In elf Fällen hatte der schwerwiegendste Angriff zudem Auwirkungen auf die Geschäftsentwicklung und bei neun Unternehmen auf die Kundenbeziehungen.

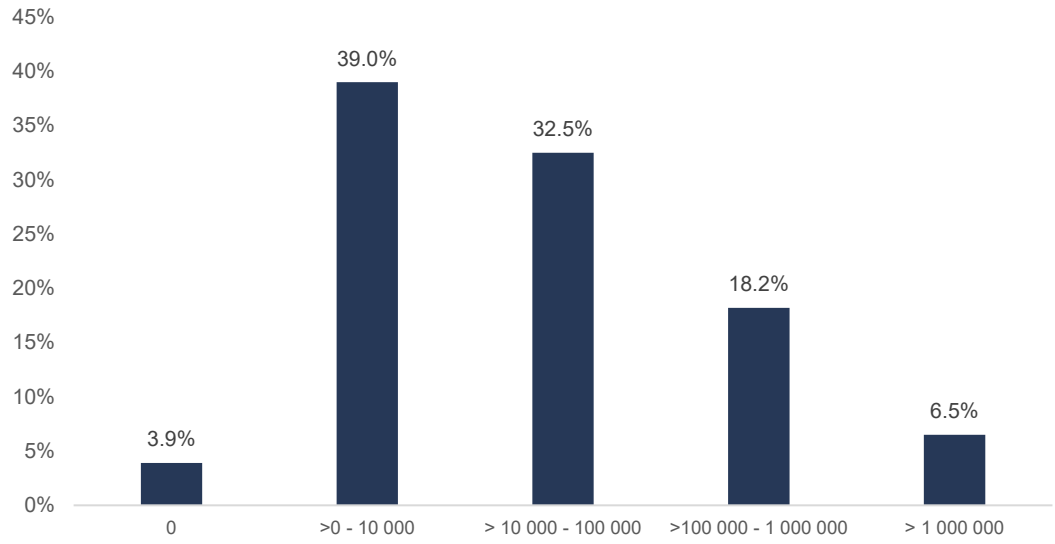
Darüber hinaus zeigen sich vor allem bei Erpressungsversuchen schwerwiegende Folgen: Jedes zwölfte Unternehmen vermeldet einen substanziellen finanziellen Schaden, der durch Ransomware ausgelöst wurde. Hinzu kommen Folgen wie Reputationsverluste, Kosten für Rechtsstreitigkeiten, Schadensersatz und Strafen sowie Umtriebe für gestohlene oder beschädigte Geräte.



Grafik 8: Nähere Angaben zum entstandenen Schaden (Mehrfachantworten möglich, N=166)

Folgekosten sprengen teilweise die Millionengrenze

Die Unternehmen wurden gefragt, welche Kosten der schwerwiegendste Angriff verursachte. Auch hier zeigt sich die grosse Bandbreite zwischen Angriffen mit relativ geringen Folgen und solchen mit schwerwiegenden Konsequenzen. Die Mehrheit vermeldete einen Schaden unter 10'000 Franken. Bei fast einem Fünftel der befragten Unternehmen verursachten die Angriffe jedoch einen Schaden zwischen 100’000 Franken und einer Million. In fünf Fällen war der Schaden gar noch grösser.

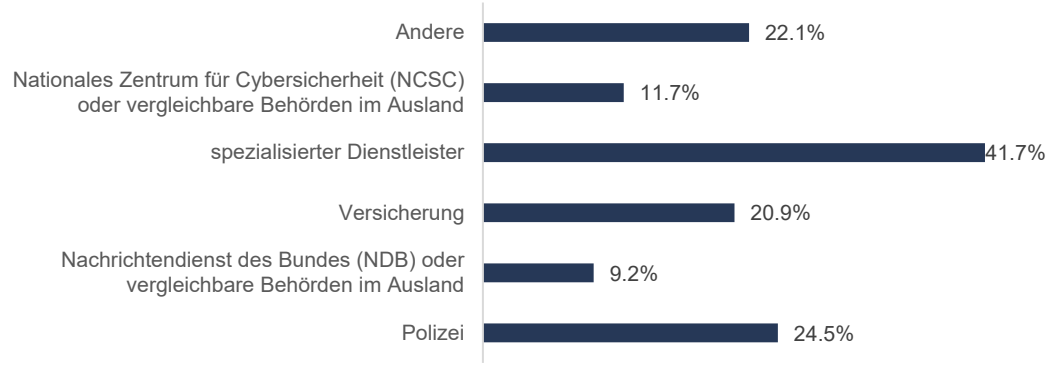


Grafik 9: Schadenshöhe kategorisiert (in Prozent; N=77)

Polizei und Behörden werden selten eingeschaltet

Am häufigsten werden nach einem schwerwiegenden Angriff spezialisierte Dienstleister aus dem Cybersicherheits-Bereich kontaktiert. Nur rund ein Viertel nimmt Kontakt zur Polizei auf. Kontakt zur Versicherung hatte rund jedes fünfte Unternehmen.

Lediglich etwa jedes neunte der befragten Unternehmen nahm nach dem Angriff Kontakt zum Nationalen Zentrum für Cybersicherheit (NCSC) oder einer vergleichbaren Behörde im Ausland auf. Hier gibt es grosses Verbesserungspotenzial – schliesslich unterstützt jede Meldung das NCSC in der Bekämpfung von Cyberkriminalität (siehe dazu Interview S. 29).



Grafik 10: Kontaktaufnahme zu Akteuren (in Prozent; Mehrfachantworten möglich; N=163)

Angriffe haben eine sensibilisierende Wirkung

Folgenschwere Angriffe sind häufig eine Zäsur in der Unternehmensgeschichte. Dabei schweissen die Angriffe die Belegschaft oft zusammen: Jedes elfte Unternehmen vermeldet, dass sich der Zusammenhalt der Mitarbeitenden nach dem Angriff erhöht hat. In vielen Betrieben hat der Vorfall zudem die Mitarbeitenden und die Geschäftsleitung für das Thema sensibilisiert.

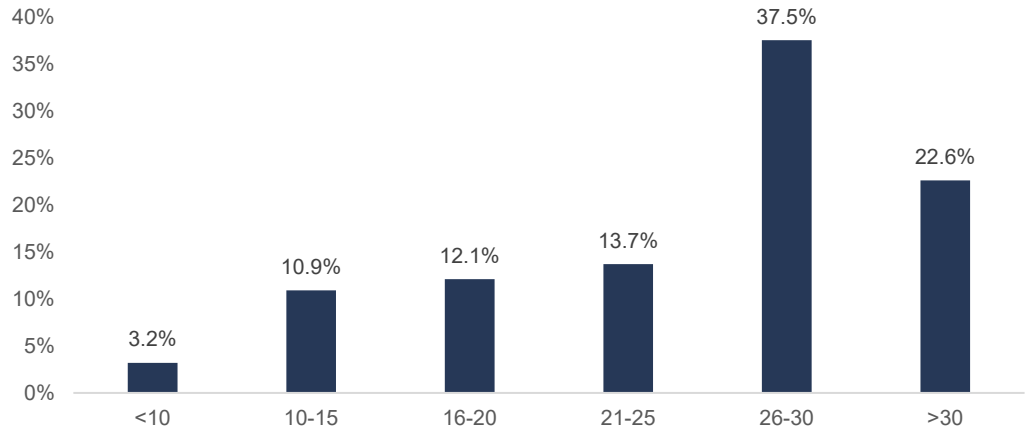
Angriffe werden häufig als Anlass für die Einführung von Awareness-Schulungen genutzt. Zudem erhöhen einige Unternehmen als Folge von Angriffen das Budget für Cybersicherheit. Auch werden die Präventionsmassnahmen nach schwerwiegenden Angriffen vielfach ausgebaut, wie im folgenden Kapitel deutlich wird.

2.4 Schutz- und Interventionsmassnahmen

Der letzte Teil des Fragebogens fokussierte auf Schutz- und Interventionsmassnahmen. Die Unternehmen wurden nach Massnahmen gefragt, mit denen sie sich gegen Angriffe schützen und zur Wehr setzen. Insgesamt standen dabei 34 verschiedene Massnahmen zur Auswahl, wobei die Unternehmen bei Bedarf noch weitere Massnahmen ergänzen konnten.

Im Durchschnitt verfügen die Unternehmen über rund 25 Massnahmen. Rund ein Viertel hat mehr als 30 Massnahmen etabliert. Grössere Unternehmen investieren in der Regel mehr in den Schutz ihrer Systeme. Fünf Firmen mit über 249 Mitarbeitenden gaben an, dass bei ihnen alle der abgefragten Massnahmen zum Einsatz kommen. Weniger als zehn Massnahmen setzen hingegen nur acht Unternehmen ein, darunter vorwiegend Firmen mit weniger als 249 Mitarbeitenden.

Grafik 11: Anzahl vorhandener Massnahmen (in Prozent; N=248)



Fast alle setzen technische Basics um

Mindeststandards im Umgang mit Cybersicherheit sind in der MEM-Industrie ganz offensichtlich weitgehend etabliert. Mit Backups, Virenschutz und Updates gehen die Unternehmen vorbildlich um. Fast 100 Prozent der befragten Firmen verfügen über folgende Massnahmen:

- Regelmässige Backups und Datensicherungen
- Aktuelle Antivirensoftware
- Schutz der ICT-Systeme mit einer Firewall
- Regelmässige und zeitnahe Installation verfügbarer Sicherheitsupdates und Patches
- Physisch getrennte Aufbewahrung von Backups

Klare Regelungen sind weit verbreitet

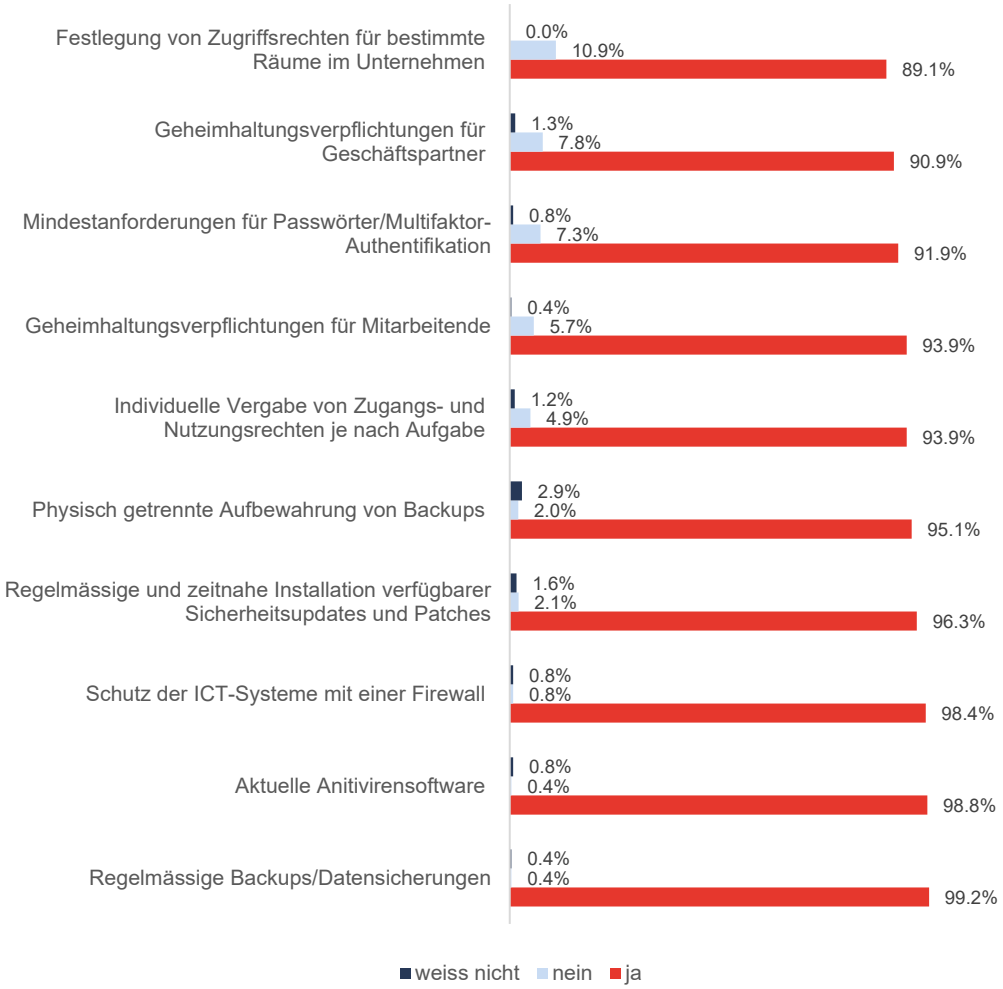
Auch klare Regelungen hat die grosse Mehrheit implementiert, etwa zu Geheimhaltung, Nutzungs- und Zugriffsrechten. Zwischen 85 und 95 Prozent verfügen über folgende Massnahmen:

- Geheimhaltungsverpflichtungen für Mitarbeitende
- Individuelle Vergabe von Zugangs- und Nutzungsrechten je nach Aufgabe
- Mindestanforderungen für Passwörter
- Geheimhaltungsverpflichtungen für Geschäftspartner
- Festlegung von Zugriffsrechten für bestimmte Räume im Unternehmen
- Besucher- und Besucherinnenmanagement bzw. Zutrittskontrollen
- Physische Sicherheitsmassnahmen wie z.B. Kameras, Alarme oder Badge- Schliesssysteme
- Klare Regelungen für den Umgang mit vertraulichen Informationen

Die meisten verfügen über Richtlinien, Notfallpläne und Schulungen

Fast 80 Prozent der Befragten setzen auf die Absicherung von Fernzugriffen für Wartung und Administration sowie auch auf eine Leitstelle und Steuerungsanlagen mit starker Authentifizierung. Ähnlich verbreitet sind Richtlinien zur ICT-Sicherheit sowie zum Notfallmanagement.

Auch Schulungen zur ICT-Sicherheit setzen mehr als drei Viertel um, ebenso wie die eindeutige Klassifizierung und Kennzeichnung von Betriebsgeheimnissen. Beim Monitoring der über das Unternehmen publizierten Informationen – etwa durch Mitarbeitende auf Social Media – ist die Umsetzungsquote ähnlich hoch.



Grafik 12: Schutz- und Interventionsmassnahmen (in Prozent; sortiert nach Häufigkeit der Nennung)

Über zwei Drittel haben strenge Kontrollen und Weisungen

Etwas grösser sind die Unterschiede mit Blick auf regelmässige Kontrollen und spezifische Weisungen. Jeweils 71 bis 72 Prozent geben an, dass sie die Einhaltung der Vorschriften regelmässig kontrollieren oder Weisungen für das Verhalten bei Messen und auf Auslandreisen erlassen. Ähnlich verbreitet sind Background-Checks von Geschäftspartnern.

Mehr als zwei Drittel setzen zudem auf regelmässige Risiko- und Schwachstellenanalysen, eine Clean-Desk-Policy, besondere Sicherheitsmassnahmen bei der Einstellung von Bewerbern sowie Übungen oder Simulationen zum Ausfall wichtiger ICT-Systeme.

ICT-Managementsysteme, Monitoring und Netzwerksegmentierung sind eher selten

Nur einige wenige Massnahmen haben sich noch nicht auf breiter Ebene etabliert. Über ein Managementsystem für die ICT-Sicherheit verfügen lediglich 64 Prozent und ein kontinuierliches Monitoring sämtlicher Log-Daten betreiben nur knapp 60 Prozent.

Etwas weniger verbreitet ist auch die Netzwerksegmentierung: Rund 55 Prozent setzen auf eine konsequente Trennung der ICT-Netzwerke, mit strikt vom Internet getrennten Bereichen. Auf die

Verschlüsselung von Festplatten und Intrusion Detection Systeme (IDS) setzt ebenfalls nur etwa die Hälfte der Unternehmen.

Mit Abstand am seltensten umgesetzt wird die Verschlüsselung von E-Mails und das Verbot des Anschlusses privater Geräte ans Firmennetzwerk. Beide Massnahmen kommen nur etwa in jedem dritten Unternehmen zum Einsatz.

Nach schweren Angriffen neu eingeführte Massnahmen

Die Unternehmen wurden befragt, welche Massnahmen sie bereits vor dem schwerwiegendsten Angriff eingeführt haben, und welche erst danach. Dabei kristallisierte sich ein Bündel von besonders beliebten Massnahmen heraus, wobei einschränkend festgestellt werden muss, dass der Grund für die Einführung nicht zwingend im genannten Angriff liegt. Jeweils 10 bis 16 Prozent der Unternehmen führten nach einer schweren Attacke eine der folgenden Massnahmen ein:

- Mindestanforderungen für Passwörter und Multi-Faktor-Authentifizierung
- Schulungen zur ICT-Sicherheit für Mitarbeitende
- Regelmässige Risiko- und Schwachstellenanalysen
- Kontinuierliches Monitoring sämtlicher Log-Daten in der Unternehmens ICT
- Schriftlich fixierte Richtlinien zum Notfallmanagement
- Intrusion Detection System (IDS)
- Einführung eines Informationssicherheits-Managementsystems

Empfehlungen aus der Praxis

3.1 Erfahrungen von Unternehmen

Geobrugg AG

Sicherheit ist das Geschäft der Geobrugg AG: Die stabilen Netze des Unternehmens schützen unter anderem vor Steinschlag. Auch bei der IT legte die Firma stets Wert auf Sicherheit – und wurde dennoch von einem Cyberangriff überrascht.

Es war ein Montagmorgen wie jeder andere. CEO Andrea Roth startete seinen Computer wollte sich an die Arbeit machen. Doch dann stellte er mit Schrecken fest: Alle Daten sind verschlüsselt – eine Cyberattacke! Dabei war die Geobrugg AG nicht unvorbereitet. Das Unternehmen aus Romanshorn hatte im Rahmen seiner Digitalstrategie auch die Cybersicherheit unter die Lupe genommen. Der Stresstest für die IT-Systeme kam schneller als erwartet und fiel überaus heftig aus.

> «Wir mussten lernen: Unser Monitoring darf am Wochenende nicht pausieren.»
>
> Andrea Roth, CEO, Geobrugg AG

Drei Tipps von Andrea Roth, CEO Geobrugg AG

01 Multi-Faktor-Authentifizierung einführen
Nach dem Angriff haben wir als erstes die dringendsten Sicherheits-Upgrades implementiert. Darauf haben wir Massnahmen, die wir bisher erst punktuell angewendet hatten, gruppenweit umgesetzt, insbesondere die Multi-Faktor-Authentifizierung.

02 Monitoring rund um die Uhr sicherstellen
Wir mussten lernen, dass das Monitoring unserer Systeme am Wochenende nicht pausieren darf. Deshalb haben wir die Überwachung der Systeme ausgelagert. Heute kümmern sich Fachleute rund um die Uhr und sieben Tage die Woche um das Monitoring.

03 Regelmässige Schulungen durchführen
Absolut entscheidend für die Cybersicherheit ist der Faktor Mensch. Unsere Mitarbeitenden sind mittlerweile für das Thema sensibilisiert – auch durch den Angriff. Doch die Angreifer lernen ständig dazu. Deshalb dürfen wir in unseren Schulungsbemühungen nicht nachlassen.

Wesco AG

Die Wesco AG wurde von Cyberkriminellen erpresst und blieb standhaft. Seither optimiert der Spezialist für Lüftung und Filtration seine Sicherheitsvorkehrungen laufend – in der Gewissheit, dass früher oder später weitere Angriffe folgen werden.

Irina Leutwyler war noch nicht lange als CEO der Wesco AG im Amt, als plötzlich ihre Fähigkeiten als Krisenmanagerin gefragt waren: Die IT-Systeme des Unternehmens aus Wettingen wurden gehackt. Die Cyberkriminellen stellten eine Lösegeldforderung, doch für die Geschäftsführerin war schnell klar, dass sie nicht darauf eingehen würde. Unter Hochdruck setzte das Unternehmen ein neues, sichereres System auf, um den Normalbetrieb wieder möglich zu machen. genommen.

> «Wer einmal angegriffen wurde, darf das Thema nicht einfach abhaken.»
>
> Irina Leutwyler, CEO, Wesco AG

Drei Tipps von Irina Leutwyler, CEO Wesco AG

01 Bei Erpressung hartnäckig bleiben
Der Lösegeldforderung stattzugeben, war für uns keine Option. Wir wollten der Finanzierung eines kriminellen Systems auf keinen Fall Vorschub leisten. Deshalb setzten wir alles daran, nicht auf die Geldforderung eingehen zu müssen.

02 Die Sicherheit des Systems verbessern
Die Wiederherstellung des Normalbetriebs hatte für uns oberste Priorität. Trotz des hohen Zeitdrucks entschieden wir uns, beim Wiederaufsetzen des Systems die Sicherheit zu erhöhen. Schrittweise haben wir ein paralleles System implementiert, das uns im Notfall absichert.

03 Immer am Thema dranbleiben
Wer einmal angegriffen wurde, darf das Thema nicht einfach abhaken. Die Systemsicherheit und die unermüdliche Sensibilisierung der Mitarbeitenden bleiben ein Dauerthema – ganz nach dem Motto «Nach dem Angriff ist vor dem Angriff».

3.2 Empfehlungen von Experten

Max Klaus
Stv. Leiter Operative Cybersicherheit beim Nationalen Zentrum für Cybersicherheit NCSC

NCSC: Informations- und Meldestelle für Cybersicherheit

Das Nationale Zentrum für Cybersicherheit NCSC ist ein Kompetenzzentrum des Bundes und gleichzeitig die offizielle Meldestelle in der Schweiz für Cyberangriffe. Für Unternehmen stellt das NCSC verschiedene Angebote bereit, darunter Warnungen und Informationen zu aktuellen Bedrohungen. Zudem bietet die Stelle Informationen und Dokumentationen für Unternehmen an, so zum Beispiel zu Standards für die Zusammenarbeit mit IT-Dienstleistern, Empfehlungen für Schutzmassnahmen und Leitfäden für den Ernstfall.
www.ncsc.admin.ch

Das Nationale Zentrum für Cybersicherheit NCSC kennt die Bedrohungslage und unterstützt Unternehmen. Max Klaus sagt, wie man sich auf den Ernstfall vorbereitet.

Wer ist für Cybersicherheit verantwortlich?
Max Klaus: Cybersicherheit ist ganz klar Chefsache. Das Thema muss regelmässig an Sitzungen der Geschäftsleitung besprochen werden. Die IT-Verantwortlichen rapportieren über aktuelle Bedrohungen und mögliche Gegenmassnahmen sowie über allfällige Restrisiken.

Wie kann man sich schützen?
Vorbereitung ist das A und O. Gut vorbereitete Unternehmen sind zwar nicht immun gegen Cyberangriffe, aber sie können die Auswirkungen massiv reduzieren.

Was gehört zu einer guten Vorbereitung?
Die wichtigsten Telefonnummern sollten ausgedruckt verfügbar sein. Ein Business Continuity Management muss etabliert sein, damit kritische Geschäftsprozesse und Schlüsselfunktionen rasch wieder verfügbar sind. Dazu gehört auch ein Krisenkommunikationskonzept.

Wie verhält man sich bei einem Erpressungsversuch richtig?
Bezahlen Sie niemals Lösegeld. Das bestärkt Cyberkriminelle nur in ihren Machenschaften. Der «Kundendienst» von professionellen Erpressern funktioniert zwar gut, aber eine Garantie auf Wiederherstellung der Daten und Entfernung der Schadware besteht nicht.

Was sollten betroffene Unternehmen stattdessen tun?
Bei Angriffen durch Cyberkriminelle sollten Sie professionelle Unterstützung in Anspruch nehmen und umgehend das Nationale Zentrum für Cybersicherheit NCSC benachrichtigen. Das hilft uns, die Bedrohungslage zu analysieren und Cyberkriminalität zu bekämpfen. Bei substanziellen Schäden ist zudem Strafanzeige zu erstatten.

> «Bezahlen Sie niemals Lösegeld.»

Drei Tipps von Levente Dobszay, InfoGuard

01 Sichern Sie Ihre Daten – und zwar richtig

Reaktions- und Wiederherstellungspläne sind eine grundlegende Voraussetzung für die digitale Überlebensfähigkeit. Neben funktionierenden Prozessen ist eine nicht kompromittierbare Datensicherung – offline und off-site – zentral. Die Funktionsfähigkeit sollte mit Wiederherstellungstests regelmässig verifiziert werden.

02 Nutzen Sie alle verfügbaren Bordmittel

Viele bestehende Mittel bleiben ungenutzt, obwohl sie die Sicherheit ohne Mehrkosten erhöhen könnten. Aktivieren Sie alle verfügbaren «Dreckfilter» in den Einstellungen und entschlacken Sie Ihre Systeme zur Verringerung der Angriffsfläche: Deaktivieren oder deinstallieren Sie nicht benötigte Elemente. Aktualisieren Sie Ihre Systeme regelmässig, um bekannte Schwachstellen zu schliessen.

03 Setzen Sie auf eine starke Authentifizierung

Der Zugang zu Systemen und Daten hängt an den digitalen Identitäten und deren Berechtigungen. Schützen Sie deshalb Ihre digitalen Identitäten und Zugangsdaten. Richten Sie unterschiedliche Benutzerkonten für unterschiedliche Aufgaben ein. Verwenden Sie wo immer möglich eine Multi-Faktor-Authentifizierung.

> «Der Zugang zu Systemen und Daten hängt an den digitalen Identitäten.»
>
> Levente Dobszay, Senior Cyber Security Consultant, InfoGuard AG

Drei Tipps von Christian Borst, Vectra AI

01 Schaffen Sie eine Security-Kultur

Der Faktor Mensch ist zentral. Schaffen Sie eine Unternehmenskultur, die Cybersicherheit und Datenschutz lebt. Sensibilisieren Sie Ihre Mitarbeitenden und investieren Sie in die Weiterbildung Ihrer IT-Verantwortlichen. Dabei geht Cybersicherheit weit über das eigne Unternehmen hinaus: Definieren Sie die Verantwortung über die gesamte Wertschöpfungskette hinweg.

02 Tauschen Sie sich mit anderen aus

Die Herausforderung Cybersicherheit müssen wir gemeinsam angehen. Ein regelmässiger Austausch mit Partnern und Lieferanten, aber auch mit anderen Unternehmen in- und ausserhalb der Branche, schafft die notwendige Basis, um die Sicherheit aller kontinuierlich zu verbessern.

03 Konzentrieren Sie sich auf das Wesentliche

Die «Basic Hygiene» ist zentral: Setzen Sie die Grundlagen eines guten IT-Betriebs konsequent um und schützen Sie Ihre digitalen Identitäten. Ein Monitoring ist wichtig, um ungewöhnliche Aktivitäten zu erkennen. Damit im Notfall rasch reagiert werden kann, braucht es ein funktionierendes Krisenmanagement. Das bedeutet auch: regelmässig üben!

> «Cybersicherheit geht weit über das eigene Unternehmen hinaus.»
>
> Christian Borst, CTO, EMEA, Vectra AI

3.3 Erkenntnisse aus Workshops

Anlässlich des Industrietags vom 23. Juni 2022 wurden mit ausgewiesenen Experten und mit den Mitgliedsfirmen von Swissmem Workshops durchgeführt. Die nachfolgenden Empfehlungen fassen die wichtigsten Erkenntnisse mit Blick auf Bedrohungslage, Auswirkungen und Schutzmassnahmen zusammen:

Bedrohungslage: Es kann jeden treffen
Es ist grundsätzlich in jedem Unternehmen der MEM-Industrie mit einem Angriff zu rechnen, der das Geschäft massiv beeinträchtigt. KMU sind in der Regel zwar weniger lukrative Ziele für gezielte Angriffe, doch auch sie sind bedroht. Die Kosten für die Bewältigung und die Umsatzverluste können für kleinere Unternehmen existenzbedrohend sein.

Mit Blick auf die IT-Architektur stellt sich die Industrie speziell dar. Sie betreibt nicht nur die übliche betriebliche Infrastruktur, sondern auch eine Infrastruktur für die Produktion. Die eingesetzten Maschinen kommen von unterschiedlichen Herstellern und sind zunehmend vernetzt. Die Heterogenität der eingesetzten Technologien erschweren das Management der Cybersicherheit.

Darüber hinaus liefern viele Unternehmen der MEM-Industrie auch Systeme oder Maschinen aus, die vernetzt sind und entsprechend geschützt werden müssen. In einer solchen Konstellation stehen die Unternehmen vor zusätzlichen Herausforderungen, wenn sie Resilienz und den Schutz sicherstellen wollen. Dabei gilt es, die gesamte Lieferkette zu berücksichtigen.

Auch ist die Industrie mit vernetzten Standorten auf der ganzen Welt besonders verwundbar. Im Workshop schilderte ein Unternehmen folgendes Beispiel: In einer Niederlassung in China wurde ein Angriff detektiert, der in Brasilien den Zugang ins Unternehmensnetzwerk gefunden hatte – zu einer Zeit, als am Hauptsitz in der Schweiz noch niemand arbeitete.

International tätige Unternehmen können ein 24/7-Monitoring dank Niederlassungen in verschiedenen Zeitzonen noch eher bewerkstelligen. Firmen mit Niederlassungen ausschliesslich in der Schweiz wird empfohlen, ein leistungsfähiges Detektions- und Reaktionssystem einzurichten, um die Nacht- und Wochenendperioden abzudecken.

Meldung ans NCSC erstatten

Das Nationale Zentrum für Cybersicherheit NCSC empfiehlt, bei schwerwiegenden Angriffen Meldung zu erstatten und Strafanzeige einzureichen. Dies hilft der öffentlichen Hand einerseits, die Bedrohungslage zu analysieren, und andererseits die benötigten Ressourcen für die Abwehr und Ermittlung bereitzustellen.

Auswirkungen: Ohne IT geht gar nichts mehr

Der Ausfall der Produktion ist für Industrieunternehmen oft der kleinere Schaden. Die Kosten für die Wiederherstellung der IT-Systeme und externe Experten wiegen schwerer. Mit zunehmender Dauer des Ausfalls verschiebt sich jedoch das Verhältnis. Je nach Marktsituation kann auch der Verlust von Aufträgen oder Kunden schmerzhaft sein.

Dabei muss es nicht zwingend der Cyberangriff selbst sein, der die IT-Systeme lahmlegt. Server werden bei Unregelmässigkeiten häufig auch als Schutzmassnahme vom Netz getrennt. Auch kann eine forensische Ermittlung oder die Überprüfung der IT-Systeme auf eine mögliche Kontamination zu mehrtägigen bis mehrwöchigen Ausfällen führen.

Unternehmen müssen im Ernstfall mehrtägige Ausfälle von ERP- und anderen IT-Systemen bewältigen können. Dabei ist auch die Hardware oft lange nicht verfügbar. Deshalb sind oft sehr kurzfristig Ersatz-Computer und andere Geräte zu beschaffen. Es empfiehlt sich deshalb eine Planung, mit welchen IT-Mitteln das Tagesgeschäft während dem Ausfall weitergeführt werden kann.

Gute Recovery-Planung reduziert die Ausfallzeit

Mit einer guten Recovery-Planung lässt sich die Ausfallzeit stark reduzieren. Eine Unterstützung durch externe Spezialisten wird sowohl für die Planung als auch für die Umsetzung empfohlen. Die Notfallplanung muss in Papierform und/oder auf einem getrennten PC verfügbar sein. Sie sollte auch definieren, wie Kunden und Lieferanten über das Ereignis informiert werden.

Schutzmassnahmen: Jede Investition lohnt sich

KMU haben bei der Umsetzung von Schutzmassnahmen in der Regel mehr Schwierigkeiten als Grossunternehmen. Das hat einerseits mit der Unternehmenskultur zu tun, andererseits aber auch mit den vorhandenen Mitteln. In einem stufenweisen Vorgehen kann ein kleineres Unternehmen zunächst identifizieren, welche Elemente der IT-Systeme den grössten Schaden verursachen können – und dort mit den Schutzmassnahmen beginnen.

Jede Investition in Schutz- und Wiederherstellungsmassnahmen reduziert den Schaden eines Angriffs. Für den effektiven Schutz der IT-Systeme ist es essenziell, die eigene Architektur im Detail zu kennen. Bei der Schutz- und Recovery-Planung sollten deshalb sowohl die eigenen IT-Spezialisten als auch externe Spezialisten – allenfalls auch solche vom Hosting – miteinbezogen werden.

Obwohl manche Unternehmen Vorbehalte gegenüber der Auslagerung von Daten haben, ist es erwiesen, dass Cloud-Lösungen deutlich sicherer sind als eigene Serversysteme. Der Aufwand, der zum Schutz dieser Systeme betrieben wird, kann durch einzelne Unternehmen niemals geleistet werden. Allerdings kommt man auch mit einer Cloud-Lösung nicht darum herum, Systeme und Schnittstellen regelmässig durch eigene Fachleute überprüfen zu lassen.

Die IT-Systeme in der Produktion haben oft eine deutlich höhere Lebensdauer als jene in den Büros. Besonders wichtig ist für Industrieunternehmen deshalb das Einrichten von sicherheitsrelevanten Zonen in der IT-Architektur, das sogenannte Zoning. Auch braucht es ein konsequentes

Konzept für das Einspielen von Patches und Updates, um Sicherheitslücken zu schliessen. Darüber hinaus werden ergänzende Investitionen in die Sicherheit empfohlen, beispielsweise in Mobiltelefone für alle Mitarbeitenden, um die Multi-Faktor-Authentifizierung zu ermöglichen.

Cybersicherheit ist eine nie abgeschlossene Aufgabe. Selbst bei umfangreichen Schutzmassnahmen muss davon ausgegangen werden, dass noch Lücken bestehen. Ein Penetration Testing durch entsprechende Dienstleister wird als Massnahme empfohlen. Da der Faktor Mensch oft das schwächste Glied in der Schutzkette ist, bieten Dienstleister auch Testangriffe über Mitarbeitende an. Die Aufarbeitung solcher Tests bewirkt einen deutlich höheren Lerneffekt als Schulungen allein.

Diese 5 Massnahmen sind ein Muss

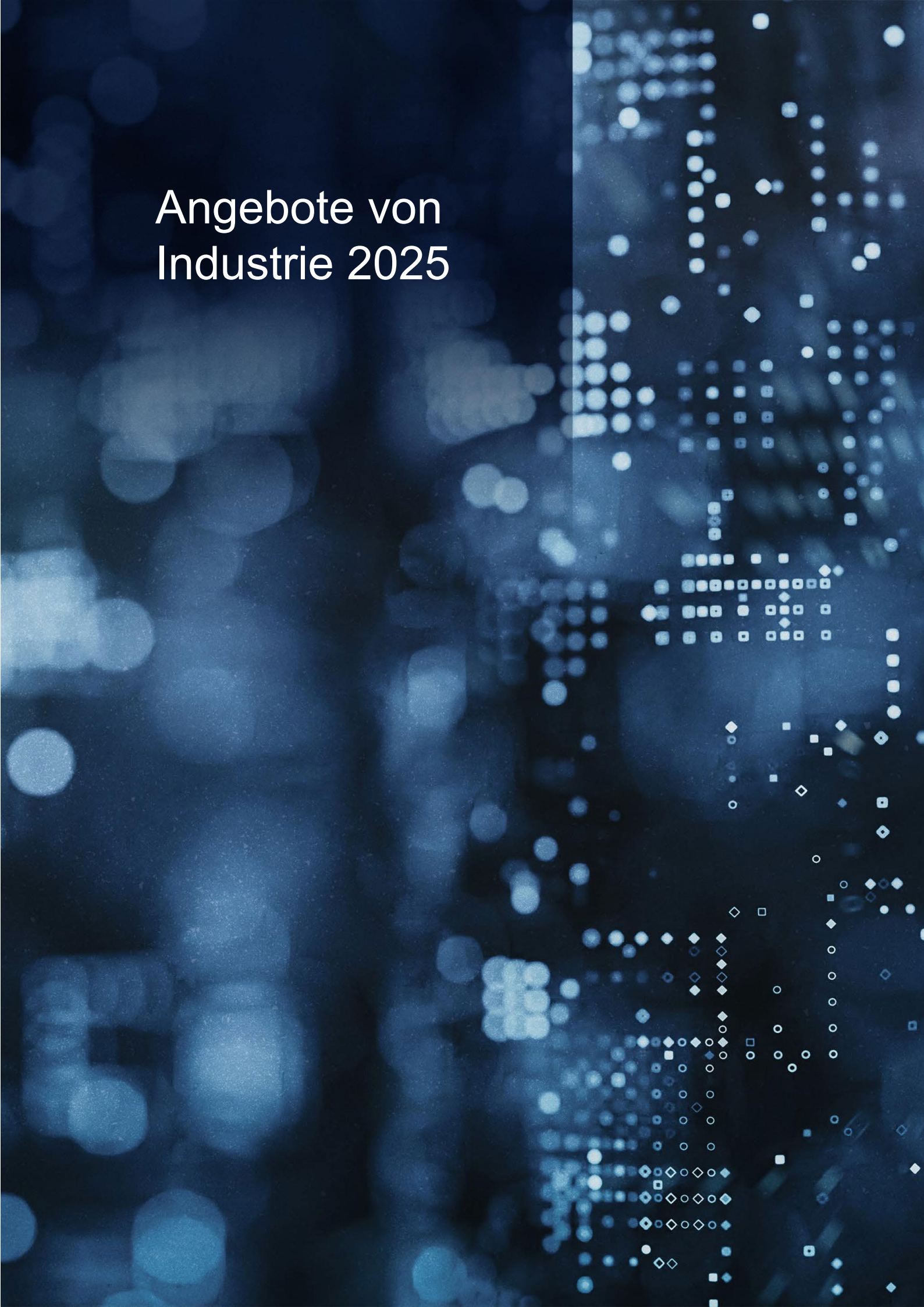
1. Multi-Faktor-Authentifizierung (MFA)
Für den Zugriff auf Konten oder Programme müssen Nutzer einen zweiten Identitätsnachweis erbringen, wie man es beispielweise vom E-Banking kennt. Bei Fernzugriffen ist dies ein Must-have, das zuverlässig vor Phishing schützt.

2. Endpoint Detection and Response (EDR)
Die «Endpunkte» des Systems – zum Beispiel auf Laptops oder Druckern – werden mit einem EDR laufend überwacht. Bei verdächtigen Aktivitäten können die betroffenen Geräte rasch vom System getrennt werden.

3. Physisch getrennte Backups
Vom firmeninternen Netzwerk physisch getrennte Backups schützen effizient vor Ransomware-Angriffen. Aber Achtung: Da dabei oft «schlafende Ransomware» mitgesichert wird, braucht es auch eine effektive Detektion.

4. Zoning
Durch das Einrichten von sicherheitsrelevanten Zonen in der IT-Architektur lässt sich diese in verschiedene Bereiche aufteilen. Dies minimiert die Angriffsfläche.

5. Patch- und Update-Management
Mit einem konsequenten Konzept für das Einspielen von Patches und Updates lassen sich Sicherheitslücken in der IT-Infrastruktur minimieren.


Angebote von
Industrie 2025

Industrie 2025 bietet Unterstützung im Bereich Cybersicherheit

Das Thema Cybersicherheit begleitet Industrie 2025 schon seit der Gründung. Durch die zunehmende Vernetzung der Infrastruktur in Produktionsunternehmen nimmt die Angreifbarkeit der Firmen kontinuierlich zu. Mit verschiedenen Aktivitäten hat sich Industrie 2025 deshalb zum Ziel gesetzt, die Cybersicherheit bei produzierenden Unternehmen erhöhen. Dabei spielen die Partner von Industrie 2025 eine wesentliche Rolle. Diese bilden das Wissensrückgrat im Themenkomplex.

Arbeitsgruppe «Cybersicherheit»

Die Arbeitsgruppen von Industrie 2025 haben das Ziel, konkrete Angebote für die wichtigsten Digitalthemen der Industrie zu erarbeiten. Dabei sind verschiedene Dienstleister und Berater rund aus dem Themenkreis vertreten, so auch in der Arbeitsgruppe «Cybersicherheit». Diese erarbeitet konkrete Hilfestellungen für Unternehmen, um die Sicherheit zu erhöhen.
Weitere Informationen finden Sie unter:
https://www.industrie2025.ch/wissen-industrie-40/arbeitsgruppen/cyber-security

Informationsplattform «Industrie 4.0 Security»

Unter www.security2025.ch hat die Arbeitsgruppe «Industrie 4.0 Security» eine Informationsplattform für das Produktionsumfeld erarbeitet. Diese besteht aus zwei wesentlichen Pfeilern:

- Leitfaden «Industrie 4.0 Security»
- Typische Anwendungsfälle im Produktionsumfeld (z.B. Fernwartung)

Workshop «Cybersicherheit»

Produzierende KMU können von einem individuellen Workshop zum Thema Cybersicherheit profitieren. Wesentliche Elemente dieses Halbtages-Workshops sind:

- Wie ernst müssen wir das Thema nehmen? (Sensibilisierung, Notwendigkeit)
- Was beinhaltet der Themenkomplex? (Übersicht, Wissensaufbau)
- Was ist unsere IST-Situation? (Analysis Canvas)
- Was sind nächste Schritte? (Hinweise auf Massnahmen, einfache Roadmap)

Der Workshop findet «on demand» statt und wird von ausgewiesenen Fachpersonen begleitet.

Weitere Informationen finden Sie hier:
https://www.industrie2025.ch/wscybersecurity

Netzwerkplattform

Die Initiative «Industrie 2025» führt Industrie 4.0-Akteure zusammen

Ob Industrieunternehmen, Lösungsanbieter oder Hochschulen – die Zusammenarbeit ermöglicht das Vorantreiben der Digitalisierung auf dem Werkplatz Schweiz.

Wissensplattform

Der Facettenreichtum von Industrie 4.0 eröffnet neue Perspektiven

Die Initiative «Industrie 2025» bündelt vorhandenes Wissen, gesammelte Erfahrungen und aktuelle Themen rund um Industrie 4.0 und stellt diese frei zur Verfügung.

Veranstaltungsplattform

Die Initiative «Industrie 2025» führt regelmässig Veranstaltungen durch

Inspiration, allgemeiner Wissensaufbau und Vernetzung der Industrie 4.0-Akteure – die Veranstaltungen dienen als wichtige Plattform für Austausch und Diskussion.

Initiative «Industrie 2025»
c/o Swissmem
Pfingstweidstrasse 102
Postfach
CH-8037 Zürich
Tel. +41 44 384 41 11
info@industrie2025.ch