ZVEI:
Die Elektroindustrie

Ergebnisbericht

Cybersicherheit: Wie sich die Automationsbranche schützt

Ergebnisse der BSI-ZVEI-Sicherheitsumfrage 2016

Zentralverband Elektrotechnik- und Elektronikindustrie

Unterstützung

Die Sicherheitsumfrage wurde durch das Bundesamt für Sicherheit in der Informationstechnik (BSI) eng in der Ausarbeitung und Durchführung unterstützt. Besonderer Dank gilt Angelika Jaschob und Thomas Häberlen.

Allianz für Cyber-Sicherheit

Der ZVEI ist Mitglied in der Allianz für Cyber-Sicherheit. Ziel der Allianz ist es, den Austausch über Vorfälle, Maßnahmen und den Stand der Technik zwischen IT-Anwendern aus der Industrie und Wirtschaft zu fördern. Mitglieder der Allianz können sich regelmäßig über die aktuelle Sicherheits- und Bedrohungslage informieren und über regionale Workshops sowie Fachkongresse beteiligen. Das BSI steht dabei als Ansprechpartner zur Verfügung. Die Mitgliedschaft ist kostenlos.

Der ZVEI ermutigt alle seine Mitgliedsunternehmen, Mitglied der Allianz für Cyber-Sicherheit zu werden.

ZVEI:
Die Elektroindustrie

Impressum

Cybersicherheit:
Wie sich die Automationsbranche schützt

Herausgeber:
ZVEI - Zentralverband Elektrotechnik- und Elektronikindustrie e. V.
Fachverband Automation
Lyoner Straße 9
60528 Frankfurt am Main

Verantwortlich:
Stefanie Gierl, Lukas Linke
Telefon: +49 69 6302-392
Fax: +49 69 6302-279
E-Mail: gierl@zvei.org, linke@zvei.org
www.zvei.org

Redaktion:
ZVEI-Lenkungskreis Automation Security

September 2016

Inhalt

Vorwort Dr. Klaus Mittelbach

September 16, 2016 - 13:05h, Cybermap Real Time Threat: GERMANY #6 Most-Attacked Country... – Die Lage ist ernst, sehr ernst sogar. Deutschland steht im Fokus von Cyberangriffen. Potenzielle Ziele gibt es viele. Politische Institutionen, kritische Infrastrukturen, Unternehmen, ja, jeder kann Ziel und Opfer von gezielten oder auch beliebigen Hacker-Angriffen werden. Die Schäden sind häufig immens, wie das Beispiel Deutscher Bundestag gezeigt hat.

Die gute Nachricht: Jeder kann sich schützen! Abwehrmaßnahmen sind effektiv, wenn sie richtig eingesetzt werden. Wichtig ist, dass ein hohes Maß an Bewusstsein für drohende Gefahren aus dem Cyberraum existiert. Wegducken geht nicht.

Cybersicherheit ist eine Grundvoraussetzung für eine erfolgreiche Digitalisierung der Wirtschaft und somit entscheidender Faktor für den Erfolg des Standorts Deutschland. Als Teil der „Allianz für Cyber-Sicherheit" ist die Erhöhung von Cybersicherheit ein zentrales Anliegen des ZVEI. Gemeinsam mit Institutionen und Unternehmen arbeiten wir daran, Wachstumsfelder wie Industrie 4.0, Energiewende oder Mobilität sicher zu gestalten.

Voraussetzung für Schutz ist Wissen. Bei unseren Mitgliedern aus der Automatisierungsbranche, einer der am stärksten vernetzt arbeitenden Wirtschaftszweige, haben wir mit dem Bundesamt für Sicherheit in der Informationstechnik (BSI) deshalb nachgefragt. Herausgekommen ist ein Sicherheitslagebild, das uns wertvolle Erkenntnisse liefert und unseren Unternehmen hilft, sich besser gegen Cyberkriminalität zu wappnen. Partnerschaftlicher Austausch und vertrauensvolle Zusammenarbeit sind hierfür unabdingbar. Mit dem vorliegenden Ergebnisbericht, den es in dieser Form zuvor nicht gegeben hat, haben wir den nächsten Schritt für mehr Sicherheit gemacht. Er hilft unseren Unternehmen, ihren Geschäften weiterhin erfolgreich nachzugehen. Weltweit.

Dr. Klaus Mittelbach
Vorsitzender der Geschäftsführung

Vorwort Arne Schönbohm

IT-Sicherheit wird immer wichtiger. Dies werden Sie, liebe Leser, die Sie im Bereich Automatisierungstechnik arbeiten, sicherlich auch in Ihrem Unternehmen, ob in Forschung, Entwicklung oder Produktion, täglich spüren – sei es nun im Zusammenhang mit Stichworten wie Industrie 4.0 oder Internet of Things, oder ganz einfach im Zusammenhang mit der normalen Office-IT.

Wie Sie in Ihren Antworten zu dieser Cybersicherheitsumfrage mitgeteilt haben, hat die Bedrohung durch Ransomware auch vor der Branche Automatisierungstechnik nicht haltgemacht. Erfreulich ist dabei, dass offenbar in den allermeisten Fällen kein gravierender Schaden entstanden ist, sondern dass die Sicherheitsmaßnahmen, die Sie bereits in Ihren Unternehmen umgesetzt haben, den Schaden in der Regel begrenzen konnten. Dies finde ich ein sehr ermutigendes Detail, denn es zeigt, dass es in der Tat etwas bringt, Schutzmaßnahmen präventiv umzusetzen.

Das BSI als die nationale Cybersicherheitsbehörde gestaltet Informationssicherheit in der Digitalisierung durch Prävention, Detektion und Reaktion für Staat, Wirtschaft und Gesellschaft. Umfragen wie die vorliegende Cybersicherheitsumfrage stellen einen wichtigen Teil dieser Arbeit dar, denn sie erlauben es dem BSI, sowohl die tatsächliche Lage von Cybersicherheitsbedrohungen als auch den Stand, den die Unternehmen bei der Umsetzung von Sicherheitsmaßnahmen erreicht haben, genauer zu messen. Auf der Basis dieser Informationen kann das BSI anschließend seine Empfehlungen zu technischem und organisatorischem Sicherheitsmanagement kalibrieren, damit einerseits die Umsetzung der Maßnahmen effizienter erfolgen kann und andererseits die empfohlenen Maßnahmen einen besseren Schutz bieten.

Die Zusammenarbeit mit Wirtschaftsverbänden wie dem ZVEI ist dabei ein sehr wichtiges Mittel. Ich möchte an dieser Stelle dem ZVEI nochmals für die Bereitschaft danken, dieses Projekt zusammen mit dem BSI durchzuführen. Aus Sicht des BSI ist es ein schöner Erfolg und ich hoffe, dass wir die Gelegenheit haben werden, die Zusammenarbeit mit dem ZVEI auf dem Gebiet Cybersicherheit in Zukunft weiter zu intensivieren.

Arne Schönbohm
Präsident des Bundesamts für Sicherheit
in der Informationstechnik

Zusammenfassung

Deutschland ist auf dem besten Weg in die digitale Gesellschaft. Für die deutsche Wirtschaft, allen voran für die Industrie, bietet die Digitalisierung der Wertschöpfung große Chancen. Doch Industrie 4.0 und digitale Produktion bieten gleichsam Angriffsfläche für Cyberkriminalität und Wirtschaftsspionage. Der Erfolg oder auch das Scheitern von Unternehmen in der digitalen Welt hängt somit entscheidend von den Investitionen in Cybersicherheit ab.

Wie gut haben sich die Unternehmen gerüstet? Als Mitglied der Allianz für Cybersicherheit und mit Unterstützung durch das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat der ZVEI 2016 die Mitgliedsunternehmen des Fachverbands Automation zum Status quo in der Cybersicherheit befragt und die Ergebnisse zusammengetragen.

An der „BSI-ZVEI-Sicherheitsumfrage 2016" haben sich 53 Unternehmen beteiligt und erstmals Auskunft über einen sensiblen Bereich gegeben. Die überwiegende Mehrheit (93 Prozent) ist international tätig, zum Teil mit eigener Fertigung im Ausland. Die Mehrzahl sind Marktführer in ihrem Segment (70 Prozent) und/oder Zulieferer eines Marktführers (42 Prozent).

Die wichtigsten Ergebnisse im Überblick:

Cybersicherheit steht für die Mehrheit der Unternehmen ganz oben auf der Agenda. 63 Prozent der Unternehmen geben an, dass dies ein Topthema der Geschäftsführungen ist.

Die Unternehmen geben durchschnittlich acht Prozent ihres IT-Gesamtbudgets für Cybersicherheit aus. Diese Investitionen decken aber nur Teilbereiche ab, darunter insbesondere die Büro-IT. Mitarbeiterschulungen und Sicherheit in der Produktionsumgebung werden als zusätzliche, wichtige Handlungsfelder gesehen.

In den meisten Fällen sind IT-Sicherheitsbeauftragte für Büro- und Produktionssysteme verantwortlich. Auf 54 Prozent der Unternehmen, die über eine derartige Position verfügen, trifft dies zu. Weitere 15 Prozent der Unternehmen haben dafür gesorgt, dass es einen Austausch gibt, wenn Prozesse beide Bereiche berühren.

54 Prozent der teilnehmenden Unternehmen verfügen nicht über eine Risikoanalyse, selbst in den Forschungs- und Entwicklungsabteilungen.

Die Top-3-Bedrohungen für die Branche sind Schadprogramme (29 Prozent der Vorfälle), menschliches Fehlverhalten (20 Prozent) und technisches Versagen (19 Prozent). Insbesondere Ransomware, wie das bekannt gewordene Locky-Programm, stellt eine Herausforderung dar.

Die meisten Angriffe erfolgen über Büro-IT-Systeme. Mitarbeiter sind mit manipulierten und speziell zugeschnittenen Viren-E-Mails wöchentlich bis täglich im Unternehmensalltag konfrontiert. Die Büroumgebung ist auch das Haupteinfallstor für komplexe, zielgerichtete Angriffe.

Sicherheitsvorfälle speziell im Produktionsbereich haben einen starken Produkt-, System- und Mitarbeiterbezug. Die häufigsten Ursachen sind Software- und Hardwareschwachstellen, Bedienungs- und Implementierungsfehler, Missbrauch, technisches Versagen und höhere Gewalt.

Insgesamt sind die Abwehrmechanismen der Unternehmen effektiv. In 70 Prozent der Vorfälle können Angriffe abgewehrt oder behoben werden, bevor ein Schaden entsteht. Dies gilt gleichermaßen für den Büro- und Produktionsbereich.

Gefahr droht durch die Hintertür. Versteckte Funktionen in Software und Geräten von Dritten sind ein zusätzliches Gefahrenpotenzial. Neun Prozent der Unternehmen stellen mindestens einmal im Monat derartige Schwachstellen in gelieferten Produkten fest.

Fazit

Das Thema Cybersicherheit ist in den Führungsetagen der Automationsunternehmen angekommen. Die Zeiten einer statischen Herangehensweise an die Cybersicherheit im Sinne eines buy and forget sind vorbei. Meist wird die Sicherheit aber noch getrennt zwischen Büro- und Produktionsumgebung organisiert. Diese Bereiche müssen noch zusammenwachsen. Die wirkliche Umgestaltung der Sicherheitsorganisation im Zuge von Industrie 4.0 steht noch bevor. Für eine anpassungsfähige, risikobasierte Einordnung der Sicherheitsmaßnahmen ist eine Asset- und Risikoanalyse unabdingbar. Auch der Faktor Mensch ist eine entscheidende Größe: Hierbei sind Detektions- und Reaktionssysteme und regelmäßige Mitarbeiterschulungen erforderlich.

Datenbasis

Die Studie: Datenbasis

Bei der BSI-ZVEI-Sicherheitsumfrage 2016 wurden 200 Mitgliedsunternehmen des ZVEI-Fachverbands Automation angeschrieben. Die Unternehmen wurden darin zu wichtigen Kennzahlen für Cybersicherheit (Benchmarking) befragt. Des Weiteren wurden die Unternehmen gebeten, konkrete Vorfälle zu beschreiben. Diese wurden ebenfalls systematisch ausgewertet (Vorfallsanalyse).

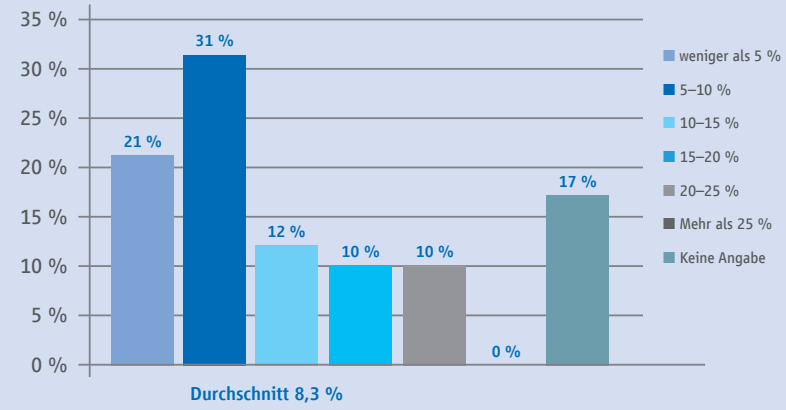
53 Unternehmen haben an der Umfrage teilgenommen, was einer Quote von 26,5 Prozent entspricht. Die durchschnittliche Antwortbasis beträgt 43 Teilnehmer (Abbrecherquote bzw. bedingte Antworten sind berücksichtigt).

Benchmarking

Was den Unternehmen die IT-Sicherheit wert ist

Wie wichtig einem Unternehmen die Cybersicherheit ist, zeigt sich unter anderem daran, wie viel Geld dafür in die Hand genommen wird. Ein zentraler Benchmarkingwert ist der Anteil der Ausgaben für IT-Sicherheit am IT-Gesamtbudget. Demnach geben die Unternehmen durchschnittlich 8,3 Prozent für ihre IT-Sicherheit aus.

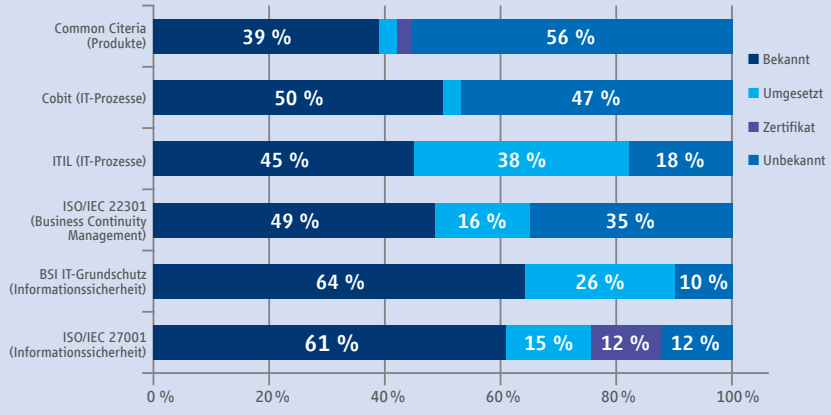
Abb. 1: Anteil IT-Security am Gesamtbudget



Quelle: ZVEI

Als Teil des IT-Gesamtbudgets konkurriert das IT-Sicherheitsbudget mit anderen Ressourcen. IT-Sicherheit allein kann die Unternehmenssicherheit nicht gewährleisten. Erforderlich sind zusätzliche Ausgaben für die physische Zutrittskontrolle und Business-Continuity-Management-Maßnahmen.

Abb. 2: Sicherheitsstandards im Büroumfeld



Quelle: ZVEI

Welches Personal für die IT-Sicherheit abgestellt wird

Zur Erreichung einer höheren Cybersicherheit in den Unternehmen sind neben finanziellen Mitteln auch die personellen Ressourcen maßgeblich. 69 Prozent der befragten Unternehmen haben einen Gesamtverantwortlichen für IT-Sicherheit. Fünf Prozent gliedern diese Position an externe Dienstleister aus, während 26 Prozent über keinen Verantwortlichen verfügen.

Bei gut der Hälfte der Unternehmen liegt die Verantwortung für die Sicherheit von Büro- wie für Produktionssysteme in einer Hand. In 54 Prozent der Unternehmen nimmt dies eine Person in Personalunion wahr, meist der CISO (Chief Information Security Officer). Bei weiteren 15 Prozent erfolgt ein Austausch, wenn sich Prozesse berühren. Ein Drittel betrachtet die beiden Unternehmensbereiche nicht gemeinsam.

Die Verbindung von Sicherheits-Know-how und Produkt- und Produktionskenntnissen wird die entscheidende Schnittstelle werden, um die Brücke zum CISO zu bauen. Für eine übergreifende Sicherheitsbetrachtung der Büro- und Produktionsumgebung ist dies zwingend erforderlich.

Wer eine Risikoanalyse durchführt

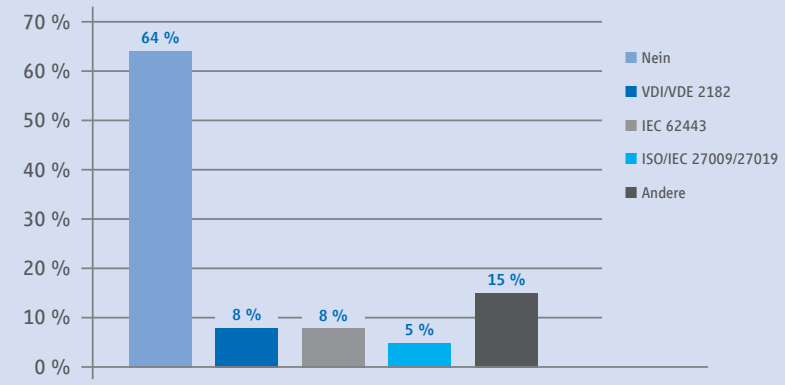
Risikoanalysen sind der erste Schritt zur Cybersicherheit. Sie machen ein abgestuftes und damit effizientes Schutzkonzept erst möglich.

54 Prozent der Unternehmen haben noch keine Risikoanalyse für die Forschungs- und Entwicklungsabteilung durchgeführt. 36 Prozent haben eine solche erstellt, zehn Prozent machen dazu keine Angaben. Für das Produktionsumfeld zeigt sich ein ähnliches Verhältnis: 41 Prozent haben eine Risikoanalyse umgesetzt. Schwerpunkte sind hier die klassischen Schutzziele: Produktionsausfall (= Verfügbarkeit, 33 Prozent der Fälle), Manipulation und Sabotage (= Integrität, 31 Prozent), Informationsdiebstahl (= Vertraulichkeit, 19 Prozent) und Auslösen einer Gefahrensituation für Menschen und Umwelt (17 Prozent).

Welche Sicherheitsstandards fürs Büroumfeld bekannt sind

Generell sind die IT-Sicherheitsstandards für das Büroumfeld hinreichend bekannt. Über 80 Prozent der befragten Unternehmen kennen die beiden gängigsten Standards für die Informationssicherheit, den IT-Grundschutz und die ISO-27000-Reihe. Allerdings setzen nur 26 bzw. 27 Prozent die Standards um.

Abb. 3: Spezielle Standards für die Produktion[1]



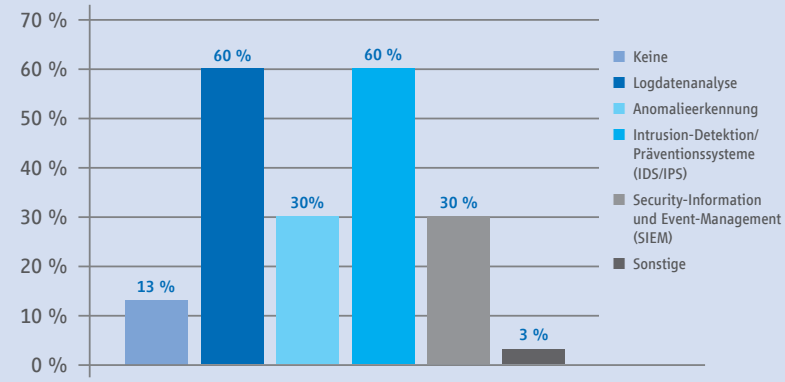
Quelle: ZVEI

Welche Sicherheitsstandards fürs Produktionsumfeld bekannt sind

In der Produktion werden konkrete Normen und Standards seltener verwendet. Erfreulicherweise orientieren sich schon acht Prozent der Automationsunternehmen an der IEC-62443-Reihe „Industrielle Kommunikationsnetze – IT-Sicherheit für Netze und Systeme", obwohl sie erst in Teilen verabschiedet ist. Der Sicherheitsstandard wird speziell für das Industrie- und Automationsumfeld entwickelt und könnte wichtige Signalwirkung für die Branche haben.

Vermutlich ist der hohe Anteil der „Nein"-Antworten darauf zurückzuführen, dass im Produktionsumfeld nur wenige Risikoanalysen durchgeführt werden. Denn die gängigen Standards für die Industrial Security schreiben die Asset- und Risikoanalyse grundsätzlich vor. Wer keine Analyse durchführt, kann folglich auch nicht die Anforderungen eines Sicherheitsstandards erfüllen.

Abb. 4: Maßnahmen zur Detektion



Quelle: ZVEI

Wie Cyberangriffe erkannt werden

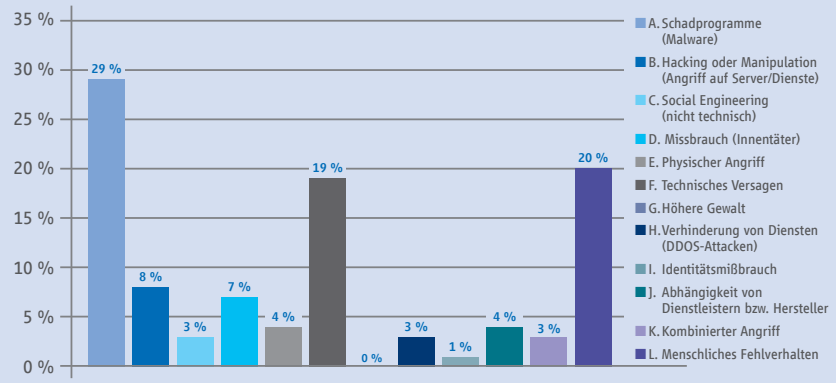
Die Mehrzahl der befragten Unternehmen (87 Prozent) setzen Detektionssysteme ein. Sie stützen sich hierbei auf die gängigen Methoden, die Logdatenanalyse sowie IDS-Systeme (jeweils 30 Prozent).

Die technischen Analysewerkzeuge müssen jedoch stets mit menschlichem Know-how hinterlegt werden. Die Schwellwerte für „False Positives" können nur in Abwägung des konkreten Unternehmenskontexts festgelegt werden. Ebenfalls sollte ein dazu ausgebildeter Mitarbeiter die Meldungen kontextbezogen interpretieren und ggf. weiterleiten.

[1] Bei der Kategorie „Andere" wurden in dem dazugehörigen Freifeld folgende Standards eingetragen: „DSAC", „ISO 9001 / TS 16949 / ISO EN14001", „ISO 9001, DIN EN60079", „iso9001 und ts16949".

Vorfallsanalyse

Abb. 5: Top-Bedrohungen



Quelle: ZVEI

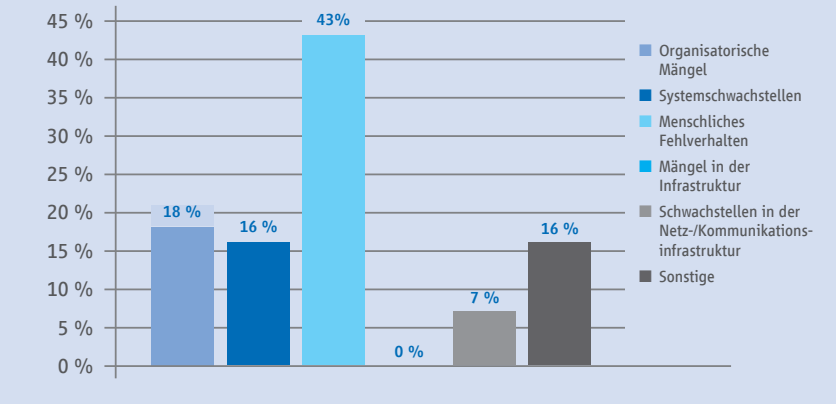
Einfallstor Büro-IT

Am gravierendsten sind Schäden durch Schadprogramme. Sie bilden 29 Prozent der von Unternehmen beschriebenen Vorfälle. Es folgen Fälle von menschlichem Fehlverhalten (20 Prozent) und technischem Versagen (19 Prozent).

Die Analyse zeigt, dass die Vorfälle und Angriffe über die Büro-IT-Systeme erfolgen und erst im Nachgang sich auf den Produktionsbereich auswirken. Gezielte Angriffe oder Schadprogramme im Produktionsbereich werden von den Unternehmen nicht genannt.

Beachtenswert sind auch die Gefährdungen, die bei komplexen Angriffen im Verbund zum Tragen kommen, nämlich die Kategorie B, C, D, K (siehe Abb. 5). Keine davon erreicht für sich allein einen hohen Wert, addiert bilden sie aber einen Anteil von 21 Prozent. Industrieunternehmen sollten sich daher auch mit diesen Szenarien intensiv auseinandersetzen.

Abb. 6: Schwachstellen



Quelle: ZVEI

Schwachstelle Mensch

Die Unternehmen wurden auch nach internen Schwachstellen gefragt, d. h. nach Aspekten, die im eigenen Verantwortungsbereich liegen und dazu beigetragen haben, dass es überhaupt zu einem Vorfall kam. Mit 43 Prozent entfällt ein Großteil der Vorfälle auf menschliches Fehlverhalten. Organisatorische Mängel (18 Prozent) und Systemschwachstellen (16 Prozent) werden dagegen deutlich seltener genannt.

Schäden werden meist rechtzeitig abgewehrt

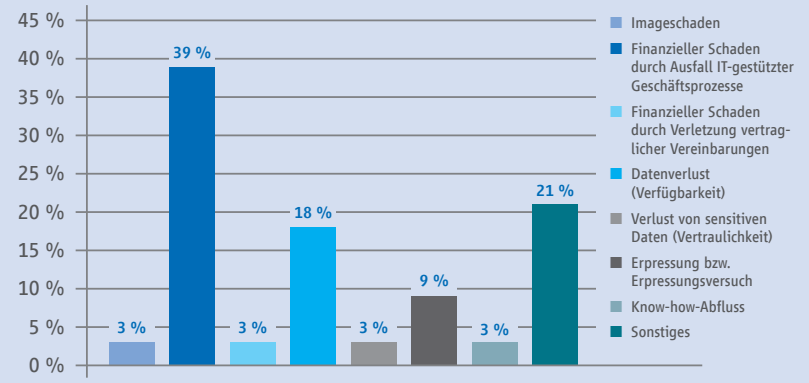
In knapp 70 Prozent der Fälle konnten Sicherheits- oder Detektionsmaßnahmen einen Schaden entweder vollständig abwehren oder zumindest den Vorfall erkennen, bevor ein Schaden entstehen konnte. Ist durch einen Vorfall ein Schaden entstanden, dann wird dieser von den Unternehmen in den meisten Fällen (96 Prozent) als unbedeutend oder begrenzt eingeschätzt. Ein Schadensfall hat meist finanzielle Einbußen (39 Prozent) und Aufwendungen für Nachsorgemaßnahmen sowie Datenverluste (18 Prozent) zur Folge. In neun Prozent der Fälle kommt es zu Erpressung oder Erpressungsversuchen.

Schadprogramme sind die größten Gefährder

In der Sicherheitsumfrage wurde zusätzlich zur qualitativen Beschreibung die Häufigkeit der gängigen Angriffswege erfasst. Schadprogramme nehmen hier eine Spitzenposition ein. Über die Hälfte der Unternehmen ist mindestens einmal im Monat von Schadsoftware etwa zum Zwecke des Betrugs betroffen. Unabhängig vom Erfolg einer solchen Attacke sollten Unternehmen im Krisenfall unverzüglich reagieren und mit den Behörden kooperieren.

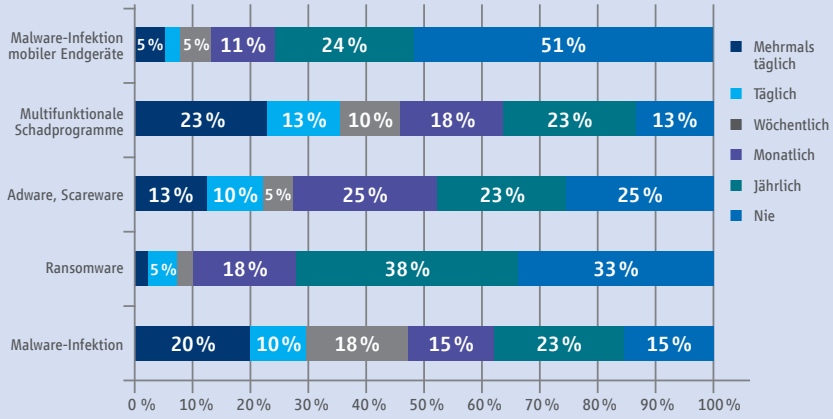
Neben den Angriffswegen wurden die Unternehmen nach internen Schwachstellen befragt, die besonders häufig ausgenutzt werden. Hier treten organisatorische Mängel deutlich als Schwerpunkt hervor.

Abb. 7: Art der entstandenen Schäden



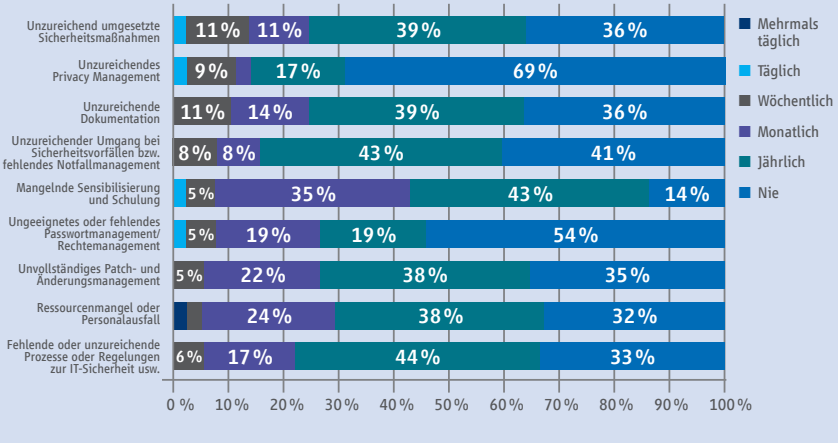
Quelle: ZVEI

Abb. 8: Häufigkeit – Schadsoftware



Quelle: ZVEI

Abb. 9: Häufigkeit – organisatorische Mängel



Quelle: ZVEI

Angriffsziel Produktion

Auch im Bereich der Produktion zeigt sich eine Reihe von Bedrohungen. Ursachen für die Vorfälle sind insbesondere:

- Software- und Hardwareschwachstellen
- Höhere Gewalt
- Technisches Versagen
- Missbrauch
- Bedienungs- und Implementierungsfehler

Es ist zu erwarten, dass durch die zunehmende Vernetzung der Produktion die Gefährdungslage und die Häufigkeit der Vorfälle in diesem Bereich zunehmen werden. Hier kann eine Risikoanalyse den Unternehmen helfen, um darauf vorbereitet zu sein.

Ausblick

Die BSI-ZVEI-Sicherheitsumfrage 2016 ist ein erster Schritt, die Unternehmen in der Automation und auch außerhalb der Branche noch stärker für Cybersicherheit zu sensibilisieren.

Der ZVEI wird im nächsten Schritt einen Orientierungsleitfaden für Komponentenhersteller erarbeiten, der den Unternehmen die Sondierung und Umsetzung der grundlegenden Sicherheitsnormen erleichtern soll.

Weitere geplante Schritte zur Erhöhung der Cybersicherheit in der Industrie sind:

- die Etablierung langfristiger Indikatoren, anhand derer die Entwicklung der Cybersicherheit gemessen und dokumentiert werden soll; dies auch in Form einer regelmäßig stattfindenden Sicherheitsumfrage
- die Schaffung von CERT- oder Austauschmöglichkeiten für Cybersicherheitsvorfälle innerhalb der Automationsbranchen und darüber hinaus.

ZVEI:
Die Elektroindustrie

ZVEI - Zentralverband Elektrotechnik- und Elektronikindustrie e.V.
Lyoner Straße 9
60528 Frankfurt am Main

Telefon: +49 69 6302-0
Fax: +49 69 6302-317
E-Mail: zvei@zvei.org
www.zvei.org