ZVEI:
Die Elektroindustrie

Öffentlicher Ergebnisbericht

Sicherheitslagebild der deutschen Elektroindustrie

Ergebnisse der BSI-ZVEI-Sicherheitsumfrage 2018

Zentralverband Elektrotechnik- und Elektronikindustrie

ZVEI:
Die Elektroindustrie

Sicherheitslagebild der deutschen Elektroindustrie

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

Verantwortlich: Lukas Linke
Telefon: +49 69 6302-432
Fax: +49 69 6302-322
E-Mail: linke@zvei.org

www.zvei.org

Juli 2018

Inhalt

Vorwort Dr. Klaus Mittelbach 4

Vorwort Arne Schönbohm 5

1. Zusammenfassung 6

2. Datenbasis 8

3. Auswertung Allgemeiner Teil 8

- 3.1 Organisation und Aufstellung der Unternehmen 9
- 3.2 Awareness 9
- 3.3 Budgets und Investitionen 10
- 3.4 Vertrauenswürdigkeit in der Lieferkette 12
- 3.5 Security-Engineering 12
- 3.6 Austausch – Allianz für Cyber-Sicherheit 13

4. Basismaßnahmen 14

5. Vorfälle und Schäden 15

- 5.1 Vorfälle 15
- 2.2 Ursachen 15

6. Strafanzeige und Kooperation mit Behörden 17

7. Ausblick 18

8. Danksagung 18

Über den ZVEI 18

Vorwort Dr. Klaus Mittelbach

Ob Zusammenarbeit oder Software: Vertrauen ist der entscheidende Faktor

Sie, liebe ZVEI-Mitglieder, haben viel geleistet. Dank Ihrer zahlreichen und detaillierten Antworten konnten wir zum ersten Mal ein ZVEI-übergreifendes Sicherheitslagebild erstellen, das zeigt, wie die Elektroindustrie in puncto Cybersicherheit aufgestellt ist. Auf dieser Grundlage lassen sich die Rahmenbedingungen für dieses Thema deutlich besser beurteilen, außerdem ermöglicht es Ihnen und dem ZVEI eine Einschätzung des aktuellen Stands der Technik. Für das entgegengebrachte Vertrauen – angesichts der zum Teil sensiblen Fragen – möchte ich mich ganz herzlich bedanken. Ihre Mühe hat sich gelohnt!

Ermutigend ist, dass das Thema Cybersicherheit definitiv in der Branche angekommen ist – 88 Prozent der Teilnehmer geben an, dass es ein Topthema der Geschäftsführung ist. Das zeigt sich auch in steigenden Budgets, die sowohl in Technik als auch in Prozesse und Know-how investiert werden. Die Ergebnisse zeigen aber auch übergreifende Herausforderungen: Die Komplexität von IT-Systemen steigt weiter, inzwischen auch auf Feldebene, also bei einzelnen Geräten und Sensoren. Gleichzeitig verstärken sich die Abhängigkeiten in der Lieferkette. Eingekaufte Hard- und Software prägt das Cybersicherheitslevel des eigenen Unternehmens sowie das der Kunden.

Das souveräne Steuern dieser Trends fällt schwerer. Als Konsequenz etablieren wir über einen Expertentag (ab 19.6.) das Thema „Vertrauenswürdigkeit in der Lieferkette“ in unserer Verbandsarbeit. Und das Sicherheitslagebild zeigt noch einen weiteren Punkt auf, bei dem es Verbesserungsbedarf gibt: Trotz vorsätzlicher Cyberattacken melden die Unternehmen diese Vorfälle nicht den Behörden, da sie die Erfolgsaussichten gering bewerten. Hier müssen wir Acht geben, dass beim Thema Cybersicherheit das Vertrauen in die staatliche Handlungsfähigkeit nicht verloren geht.

Dies bestärkt den ZVEI darin, sich für eine intensivierte europäische und internationale Zusammenarbeit bei der Verfolgung von Cyberkriminalität einzusetzen. Die Allianz für Cyber-Sicherheit ist hierfür die richtige Plattform. Sie bündelt Expertenwissen und bietet kostenlos Hilfestellung für Unternehmen sowie eine vertrauensvolle Umgebung für den Austausch über den Umgang mit Cyberattacken.

Das Sicherheitslagebild zeigt: Vertrauen ist der entscheidende Faktor – ob in puncto sichere Drittprodukte von Security-Anbietern oder bei der Zusammenarbeit zwischen Industrie, Behörden und Kunden. Daran müssen wir jetzt arbeiten – denn mehr Cybersicherheit in der Elektroindustrie lässt sich nur mit dem nötigen Vertrauen gewährleisten.

Ihr
Dr. Klaus Mittelbach
Vorsitzender der Geschäftsführung

Vorwort Arne Schönbohm

Die Digitalisierung ist in vollem Gange. Sie kann aber nur dann gelingen, wenn Cybersicherheit von vornherein ganzheitlich mitgedacht wird. Wenn wir die Digitalisierung zukunftssicher gestalten und die Widerstandsfähigkeit Deutschlands gegen Cybergefahren erhöhen wollen, dann müssen wir die damit verbundenen Herausforderungen angehen. Als nationale Cybersicherheitsbehörde und zentrales Kompetenzzentrum für Cybersicherheit in Deutschland nehmen wir diese Aufgabe an, in intensiver Zusammenarbeit mit allen relevanten Akteuren in Staat, Wirtschaft und Gesellschaft. Die Cyber-Sicherheitsstrategie der Bundesregierung gibt das klare Ziel vor, eine gesamtstaatliche Cybersicherheitsinfrastruktur zu schaffen, die leistungsstark und nachhaltig ist. Der Koalitionsvertrag der Bundesregierung sieht eine Stärkung und einen Ausbau der nationalen Cyber-Sicherheitsbehörde BSI vor.

Dass dies dringend notwendig ist, zeigt ein Blick auf die aktuelle Gefährdungslage, die auf hohem Niveau angespannt ist. Unentdeckte Sicherheitslücken oder die täglich rund 280.000 neuen Schadsoftware-Varianten bieten Cyberangreifern weitreichende Möglichkeiten, Informationen auszuspähen, Geschäfts- und Verwaltungsprozesse zu sabotieren oder sich auf Kosten Dritter kriminell zu bereichern. Begünstigt wird diese Entwicklung durch die voranschreitende Vernetzung von Systemen und Geräten, etwa im Rahmen der Industrie 4.0 oder dem Internet der Dinge. Zudem agieren Angreifer zunehmend professionell und nutzen ausgefeilte Angriffsmethoden, die schwer zu entdecken und nicht mit klassischen Schutzmechanismen wie Virenscannern und Firewalls abzuwehren sind.

Grundlage einer effektiven Cyberabwehr ist ein möglichst umfassendes und aktuelles Lagebild. Als nationale Cybersicherheitsbehörde erstellt und pflegt das BSI eigene Lagebilder, die wir unseren Zielgruppen in Staat, Wirtschaft und Gesellschaft zur Verfügung stellen. Zudem unterstützt das BSI Partner wie den ZVEI bei der Erstellung branchen- oder themenbezogener Lagebilder. Ausgehend von einem aktuellen Lagebild können Verwaltung, Wirtschaft und Wissenschaft mit Informationen versorgt werden, die zur Schaffung eines angemessenen Cybersicherheitsniveaus in diesen Organisationen beitragen. Lagebilder schaffen mehr Transparenz über aktuelle Angriffsformen und Schwachstellen in relevanten IT-Produkten und leiten daraus Empfehlungen zu notwendigen Sicherheitsmaßnahmen ab.

Das vorliegende Branchenlagebild ist ein Ergebnis der langfristigen und fruchtbaren Zusammenarbeit von ZVEI und BSI. Es liefert einige wertvolle Einblicke und Erkenntnisse, die Ihnen beim Schutz Ihrer IT vor Cyberangriffen gute Dienste leisten können.

Arne Schönbohm,
Präsident des Bundesamts für Sicherheit
in der Informationstechnik (BSI)

1 Zusammenfassung

Hohe Management-Awareness für Cybersicherheit:

Inzwischen haben 87 Prozent der Teilnehmer mindestens einen Hauptverantwortlichen für IT-Sicherheit im Unternehmen. Dazu geben 88 Prozent der Teilnehmer an, dass Cybersicherheit ein Topthema in der jeweiligen Geschäftsführung ist. Um dies zu konkretisieren wurde gefragt, wie häufig sich die Geschäftsführung zur Cybersicherheit berichten lässt und/oder Lageberichte bespricht: 31 Prozent tun dies regelmäßig, weitere 42 Prozent besprechen dies in größeren Abständen. Cybersicherheit ist somit fest auf Entscheiderebene etabliert.

Basismaßnahmen der IT-Sicherheit werden umgesetzt:

Die Teilnehmer setzten wichtige Basismaßnahmen wie Back-up (98 %), Patch-Management (94 %), Malware-Abwehr (98 %) und VPN-Verschlüsselung (98 %) in der Breite um. Auch weiterführende Maßnahmen wie Black- und Whitelisting (90 %) sowie der Einsatz von Sicherheits-Gateways (88 %) sind für die Office-IT-Systeme etabliert. Diese Maßnahmen legen ein gutes Fundament, um robuste Schutzmechanismen aufzubauen.

Budgets für Cybersicherheit steigen:

42 Prozent der Teilnehmer werden in den zwölf bis 18 Monaten ihr Budget für Cybersicherheit erhöhen. Lediglich ein Prozent rechnet mit sinkenden Budgets. Der ZVEI empfiehlt in Anlehnung an die Vorgabe für Bundesbehörden, mindestens zehn Prozent des IT-Budgets für Cybersicherheit zu investieren. Ob dieses Ziel durch die Budgeterhöhungen im Durchschnitt erreicht wird, lässt sich noch nicht feststellen. Insgesamt unterstreicht es die Bedeutung des Themas, dass die Unternehmen bereit sind, breit in ihre Sicherheit zu investieren.

Security-Anbieter müssen besser werden:

Unternehmen stoßen auf unerwartet viele Hindernisse am Markt, wenn sie bereit sind, in Cybersicherheit zu investieren. Leider unverändert stellt für 25 Prozent der Teilnehmer der Fachkräftemangel das größte Hindernis dar. Bemerkenswert sind jedoch die Angaben in Richtung der Anbieter: 17 Prozent geben die Inkompatibilität der Security-Lösungen mit Bestand als Hindernis an, weitere 15 Prozent die eigentliche Qualifizierung der Anbieter und zusätzliche acht Prozent finden keine Produkte für ihr Security-Anliegen. Vor diesem Hintergrund sind die Anbieter aufgefordert, für mehr Qualität, Transparenz und Kundennähe zu sorgen.

Security-Engineering vielerorts aufgesetzt, aber noch kein Standard:

17 Prozent der Unternehmen haben ein Security-Engineering für nahezu alle Produkte eingeführt. Weitere 21 Prozent geben an, dies für einzelne Produkte getan zu haben und 16 Prozent wollen dies in naher Zukunft tun. Somit haben knapp über die Hälfte der Teilnehmer erste Prozesse aufgesetzt, um Security by Design auch umzusetzen. Der ZVEI wird bei künftigen Umfragen diesen Faktor weiter beobachten, da ein breiter „Security by Design/Default"-Ansatz ein Kernelement der Digitalisierung ist.

Software-Schwachstellen fordern die Office- und Produktions-IT heraus:

Auf die Frage, welcher Faktor zum Eintritt eines gravierenden Sicherheitsvorfalls beitrug, zeigen sich für die Office- und Produktions-IT vergleichbare Top-3-Ursachen:

Bemerkenswert ist, dass im Bereich der Produktions-IT die fehlende Qualität und geringe Manipulationssicherheit von eingekaufter oder selbst entwickelter Software häufiger Ursache eines gravierenden Sicherheitsvorfalls ist als der „Faktor Mensch". Bedenkt man, dass Software auf allen Industrieebenen (Embedded, Feld, Steuerung, MES und ERP) an Bedeutung gewinnt, macht dies einen klaren Handlungsauftrag für die Branche deutlich. Die zentrale Frage für die Unternehmen ist, wie sich die zunehmende Komplexität der IT-Systeme managen lässt.

Office-IT	Produktions-IT
Menschliches Fehlverhalten 58 % Schwachstellen in der Software 25 % Organisatorische Mängel 8 %	Schwachstellen in der Software 29 % Menschliches Fehlverhalten 22 % Organisatorische Mängel 19 %
Angaben: Ursachenverteilung bezogen auf alle genannten gravierenden Sicherheitsvorfälle.	

Die Vertrauenswürdigkeit von Drittprodukten wird zum Branchenthema:

Eingekaufte Hard- und Software darf nicht die eigene Sicherheit oder die der eigenen Kunden gefährden. Die Integrität, Verlässlichkeit und Cybersicherheit (= Vertrauenswürdigkeit) der Drittprodukte zu bewerten und sicherzustellen, ist jedoch eine große Herausforderung. So geben 39 Prozent der Teilnehmer an, dass Vertrauenswürdigkeit eine hohe Relevanz für das Unternehmen hat. Weitere 19 Prozent setzen Maßnahmen im Bereich Qualitätsprüfung, Supply-Chain-Management oder Product-Security um. Als Konsequenz wird der ZVEI das Thema Vertrauenswürdigkeit und Cybersicherheit in der Lieferkette als Branchenthema verankern.

Elektroindustrie von den gängigen Bedrohungen betroffen:

Eine besondere oder abweichende Bedrohungslage ist für die Elektroindustrie nicht festzustellen. Wie andere Sektoren waren 60 Prozent der Unternehmen vor allem von Ransomware und Verschlüsselungstrojanern betroffen. Der CEO-Betrug (Geldüberweisungen auf Basis von gefälschten CEO-Aufträgen) führte bei sechs Prozent der Teilnehmer zu Sicherheitsvorfällen. Auch dies deckt sich mit den Ergebnissen des BSI-Sicherheitslagebilds 2017. Oftmals können die Vorfälle ohne größere Finanzschäden gelöst werden. Wenn jedoch gravierende Vorkommnisse geschehen, führt dies durchaus zu hohen Schadenssummen. So geben neun Prozent der Teilnehmer an, in den vergangenen zwei Jahren einen Schaden von 100.000 Euro oder höher erlitten zu haben. Insbesondere für mittelständische Unternehmen ist dies bereits eine erhebliche Belastung.

Geringes Vertrauen in erfolgreiche Ermittlungen:

Selbst wenn die Unternehmen bereits von einer vorsätzlichen Straftat ausgehen, sind 83 Prozent nicht bereit, eine Strafanzeige aufzugeben. Bezüglich der Hinderungsgründe erwähnen nur zwei Prozent die oft vermutete Angst für Reputationsschäden. Viel eher wird auf die geringe Aussicht auf Erfolg (21 % aller Antworten) und die Nichtzuständigkeit der Polizeibehörden verwiesen, da der/die Täter im Ausland vermutet werden (weitere 20 %). Es zeigt sich eine bereits fest etablierte Skepsis dem staatlichen Handlungsvermögen gegenüber. Entsprechend müssen die internationalen Kooperationen zur Bekämpfung von Cybercrime ausgebaut und es muss stärker über erfolgreiche Ermittlungen kommuniziert werden.

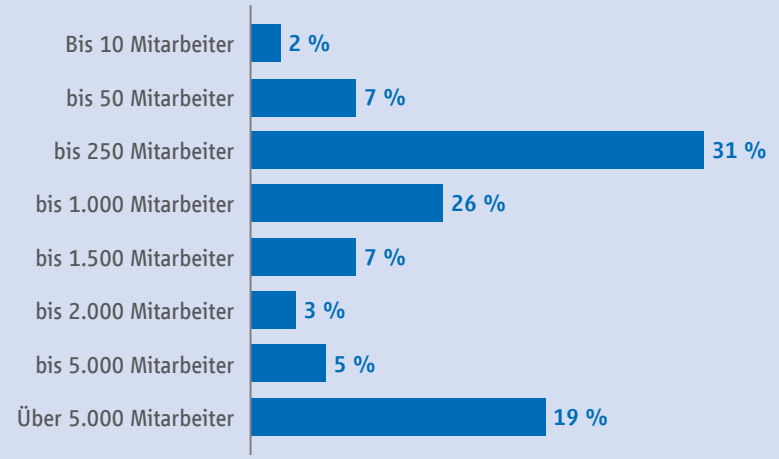
2 Datenbasis

An der Umfrage nahmen 101 ZVEI-Mitglieder aus 21 Sektor-Fachverbänden teil. Angesichts der insgesamt ca. 1.600 ZVEI-Unternehmen sind die Ergebnisse daher im statistischen Sinne nicht repräsentativ. Jedoch ermöglichen sie einen ernstzunehmenden Einblick in die Realitäten der Elektroindustrie. Nicht alle Fragen wurden von allen Teilnehmern beantwortet, sodass die durchschnittliche Antwortbasis der nicht bedingten Fragen 73 Unternehmen beträgt.

Unternehmensgröße:

Es haben mehrheitlich KMUs mit bis zu 1.000 Mitarbeitern teilgenommen (siehe Abbildung Frage 1). Die Konzernebene ist mit 19 Prozent der Teilnehmer charakteristisch für die Branche vertreten. Für die Auswertung der Umfrage ist das von Bedeutung, da Konzerne hinsichtlich der Ressourcen und Fähigkeiten besser aufgestellt sind. Sie können auf Vorfälle reagieren und haben meist Security-Prozesse etabliert. Insofern kann ein hoher Konzernanteil die Ergebnisse verzerren, indem die Antworten positiver scheinen, als dass es der Realität entspricht. Das Teilnehmerbild der ZVEI-Umfrage ermöglicht jedoch eine sehr gute Deutung und Übertragung der Ergebnisse.

Frage 1: Wie viele Mitarbeiter beschäftigt Ihr Unternehmen?



Quelle: ZVEI

Antwortgeber:

Im Regelfall haben die IT- und Sicherheitsverantwortlichen (CIOs, CISOs, Leiter IT-Abteilung, Zuständiger für das Unternehmensnetzwerk) in Abstimmung mit den Kollegen die Fragen beantwortet. In Einzelfällen führten Verantwortliche für die Produktions-, Produkt- und Lösungssicherheit (im Sinne der Security) die Umfrage durch.

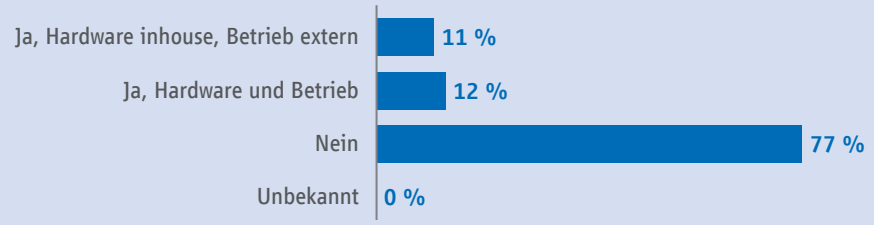
3 Auswertung Allgemeiner Teil

3.1 Organisation und Aufstellung der Unternehmen

Abfrage: Gibt es einen Hauptverantwortlichen für die IT-Sicherheit in Ihrem Unternehmen?

Inzwischen haben viele Unternehmen Rollen und Verantwortliche für Cybersicherheit geschaffen. 87 Prozent der Teilnehmer geben an, mindestens einen Hauptverantwortlichen für IT-Sicherheit benannt zu haben. Dies ist ein erfreulicher Wert, da der wichtigste erste Schritt für Cybersicherheit ist, Prozesse und Zuständigkeiten aufzusetzen. Cybersicherheit lässt sich nicht allein durch technische Mittel erreichen, zumal die Maßnahmen fortwährend dem Stand der Technik sowie im Hinblick auf die Bedrohungslage hin angepasst werden müssen. Das Investment in Menschen ist essenziell.

Frage 2: Wird Ihre IT durch einen Dienstleister verwaltet?

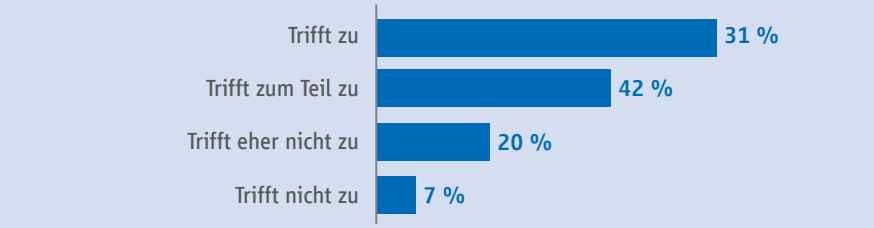


Quelle: ZVEI

3.2 Awareness

Cybersicherheit muss top-down durch die Entscheiderebene mandatiert und unterstützt werden. Andernfalls können die notwendigen Budgets und Prozesse nicht umgesetzt werden. Cybersicherheit hat Auswirkungen auf die gesamte Organisation. Vor diesem Hintergrund ist es erfreulich, dass 88 Prozent der Teilnehmer antworten, dass Cybersicherheit ein Topthema in der jeweiligen Geschäftsführung ist. Um dies zu konkretisieren wurde gefragt, wie häufig sich die Geschäftsführung zur Cybersicherheit berichten lässt und/oder Lageberichte bespricht: 31 Prozent tun dies regelmäßig, weitere 42 Prozent besprechen dies in größeren Abständen. Inwiefern daraus konkrete Handlungen abgeleitet und freigegeben werden, ist in Zukunft zu prüfen.

Frage 3: Die Geschäftsführung nimmt Lageberichte zur IT- und Cybersicherheit der Behörden und Security-Community aktiv auf.



Quelle: ZVEI

Ein weiterer Aspekt der Awareness ist die Kenntnis des BSI-IT-Grundschutzes. Der IT-Grundschutz kann als Maßstab für die Bestimmung des Stands der Technik herangezogen werden. Traditionell bezieht er sich auf die Themen der Informationssicherheit (siehe ISO-2700x-Reihe) sowie Netzwerk- und Kommunikationssicherheit. Der BSI-Grundschutz wird jedoch über einzelne Module auch mit Automations- und Industriethemen ergänzt (siehe Module für Industriesteuerungsanlagen, Sensoren und Aktoren). Er gewinnt damit als Orientierungspunkt immer mehr Relevanz für produzierende Industrieunternehmen.[1]

Abfrage: Kennen Sie die überarbeitete Version des BSI-Grundschutzes?

Über die Hälfte der Teilnehmer kennt die überarbeitete Version des Grundschutzes (53 %). 47 Prozent der Unternehmen ist er unbekannt. Der ZVEI wird diesen Wert bei nachfolgenden Umfragen weiterverfolgen und die Bekanntheit des Grundschutzes fördern.

[1] Weitere Hinweise siehe: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/itgrundschutz_node.html

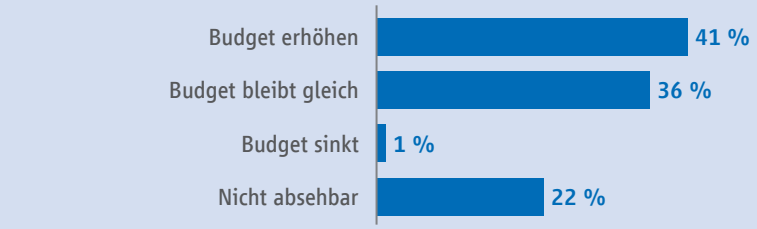
3.3 Budgets und Investitionen

Ein weiterer Faktor, mit dem sich der Stellenwert der Cybersicherheit in den Unternehmen testen lässt, ist die Frage, ob diese bereit sind zu investieren. Maßnahmen in Personal, Technik und Prozesse erfordern unweigerlich erhebliche Ressourcen.

Abfrage: Plant Ihr Unternehmen eine Veränderung des Budgets für Cybersicherheit in den nächsten zwölf bis 18 Monaten?

Anscheinend materialisiert sich die hohe Awareness im Management auch in den Budgets. 42 Prozent der Unternehmen geben an, dass sie mit steigenden Budgets rechnen. Lediglich ein einziges Unternehmen geht von sinkenden Investitionen aus. Das jeweilige Ausgangsniveau wurde nicht abgefragt. Der ZVEI empfiehlt in Anlehnung an die Vorgabe für Bundesbehörden, mindestens zehn Prozent des IT-Budgets für Cybersicherheit zu investieren.

Frage 4: Plant Ihr Unternehmen eine Veränderung des Budgets für Cybersicherheit in den nächsten 12–18 Monaten?

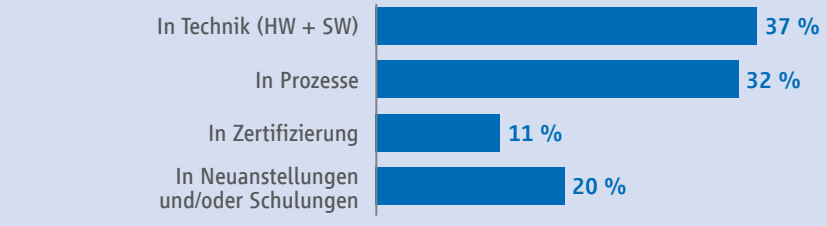


Quelle: ZVEI

Abfrage: Wenn Sie Investitionen in Cybersicherheit vornehmen würden, in welche Bereiche würden Sie primär investieren?

Cybersicherheit lässt sich nicht im Regal kaufen. Eine einmalige Investition in Technik reicht nicht aus. Kompetentes Personal muss Soft- und Hardware implementieren, betreiben, warten und auf Veränderungen reagieren können. All dies sollte dokumentiert und mit Partnern und Kunden geteilt werden können, um auch im Krisenfall handlungsfähig zu sein. Daher ist es neben dem „ob" auch entscheidend zu wissen, in was die Unternehmen im Bereich der Cybersicherheit investieren. Diesbezüglich sind die Ergebnisse ermutigend. In das gesamte Spektrum von Technik, Personal, Prozessen und Zertifizierung wird investiert. Die Unternehmen haben erkannt, dass man einen holistischen Ansatz wählen muss, um Cybersicherheit robust aufzubauen.

Frage 5: Wenn Sie Investitionen in Cybersicherheit vornehmen würden, in welche Bereiche würden Sie primär investieren?

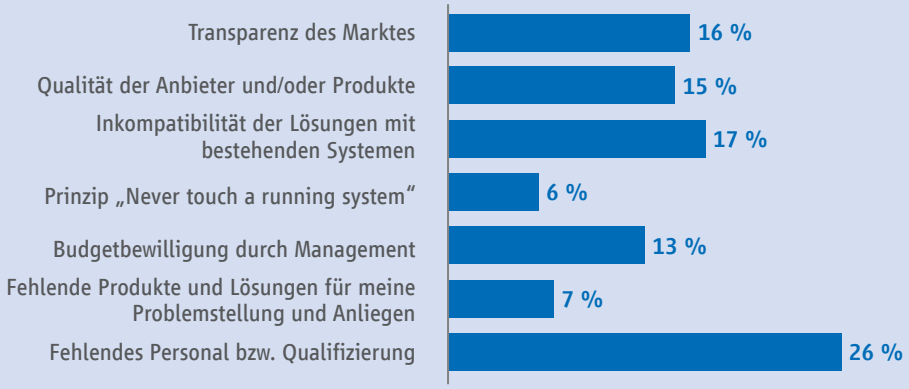


Quelle: ZVEI

Abfrage: Wenn Sie Investitionen in Cybersicherheit vornehmen wollten, worin sähen Sie die größten Hindernisse?

Bemerkenswert ist, dass die Investition in Cybersicherheit den Unternehmen schwerer fällt, als dass dies der Fall sein sollte. Die Nennung des Fachkräftemangels (sehen 25 % als Hindernis) ist nicht überraschend, denn dieser hemmt wie in anderen Sektoren die Entwicklung. Drei Kennzahlen sind jedoch aus Sicht des ZVEI hervorzuheben. Wenn Unternehmen investieren wollen, stellt sich der Markt als zu intransparent dar (sehen 16 % als Hindernis), finden die Betroffenen nicht die passende Lösung für ihr Problem (8 %) und stellen weitere 17 Prozent der Teilnehmer fest, dass die beworbene Lösung im Anschluss inkompatibel zu ihrem bestehenden System ist. Das sind ernstzunehmende Probleme und ein Auftrag an die Security-Anbieter, zielgenauer auf die Bedürfnisse der Anwender aus der Elektroindustrie einzugehen. Mangelnde Lösungskompetenz darf nicht zum „Showstopper" für Cybersicherheit werden.

Frage 6: Wenn Sie Investitionen in IT-Sicherheit vornehmen wollten, worin sähen Sie die größten Hindernisse?



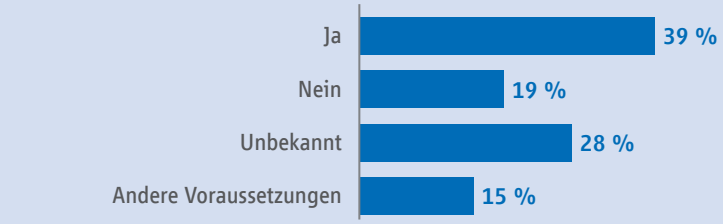
Quelle: ZVEI

3.4 Vertrauenswürdigkeit in der Lieferkette

Abfrage: Ist das Thema Vertrauenswürdigkeit von Drittprodukten relevant für Ihren Einkauf bzw. Ihr Supply-Chain-Management?

Die Komplexität von IT-Systemen steigt immer weiter. Das Management von wechselseitigen Auswirkungen stellt die Unternehmen vor Herausforderungen. Da viele ZVEI-Mitglieder Verbundkomponenten und -systeme mit eingekaufter Hard- und Software herstellen, ist die Verlässlichkeit, Integrität und Manipulationssicherheit der Drittprodukte von großer Bedeutung. Drittprodukte dürfen nicht durch Schwachstellen die eigene Sicherheit oder die der eigenen Kunden gefährden. Bereits 19 Prozent der Unternehmen geben an, dass sie Maßnahmen zur Gewährleistung der Vertrauenswürdigkeit planen oder umsetzen. Weitere 39 Prozent sagen, dass das Thema für sie eine hohe Relevanz besitzt. Inwiefern dies zu Maßnahmen führt, bleibt jedoch offen.

Frage 7: Ist das Thema Vertrauenswürdigkeit (i.S.v. Manipulationsschutz und Freiheit von nicht dokumentierten Funktionen) von Drittprodukten relevant für Ihren Einkauf bzw. Ihr Supply Chain Management?



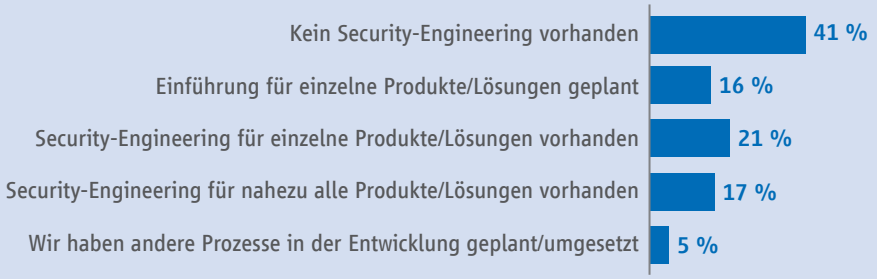
Quelle: ZVEI

3.5 Security-Engineering

Abfrage: Haben Sie ein Security-Engineering eingeführt?

Die Umsetzung von Security by Design wird zu einer wesentlichen Anforderung an Konsum- und Industrieprodukte. Dies kann nur durch ein Security-Engineering mit Leben gefüllt werden. Konkrete Anforderungen, Prozesse und Testverfahren müssen dafür bei der Produktenwicklung und -fertigung berücksichtigt werden. Insofern ist es bemerkenswert, dass 41 Prozent der Teilnehmer angeben, kein Security-Engineering zu haben. Lediglich 17 Prozent implementieren es für fast alle Produkte. Da die Einführung eines derartigen Engineering komplex und zeitaufwendig ist, ist es gleichwohl verständlich, dass die Mehrzahl der Teilnehmer die Einführung zunächst für einzelne Produktgruppen vorsieht. Grundsätzlich gilt jedoch, dass die Branche, wenn sie Security by Design als Qualitäts- und Differenzierungsmerkmal etablieren möchte, größere Anstrengungen unternehmen muss.

Frage 8: Haben Sie ein Security-Engineering eingeführt?



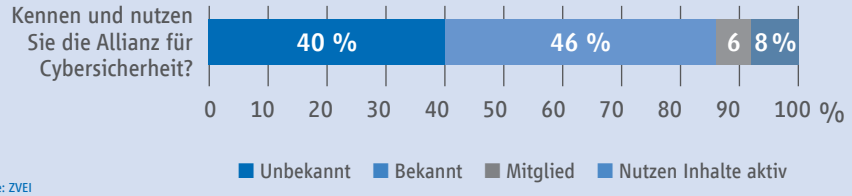
Quelle: ZVEI

3.6 Austausch – Allianz für Cyber-Sicherheit

Abfrage: Kennen und nutzen Sie die Allianz für Cyber-Sicherheit?

Kein Unternehmen kann die Herausforderungen für die Unternehmens-, Anlagen- und Produkt-Security allein bewerkstelligen. Der Austausch über Schwachstellen, Trends und Best Practices unterstützt die eigenen Arbeiten ungemein. Die Allianz für Cyber-Sicherheit (ACS) ist das größte Informations- und Austauschnetzwerk in Deutschland. Es wird getragen vom Bundesinnenministerium und Bundesamt für Sicherheit in der Informationstechnik und kann dadurch kostenlos Analysen, Hilfestellungen und Expertenkreise für mittelständische Unternehmen bereitstellen.[2] Angesichts des Leistungsspektrums der ACS ist die geringe Mitgliederquote der ZVEI-Unternehmen unverständlich. Der ZVEI empfiehlt allen seinen Mitgliedsunternehmen, Mitglied in der kostenfreien ACS zu werden, um einen hilfreichen Informationsaustausch sicherzustellen. Als Reaktion auf die Ergebnisse wird der ZVEI die Ansprache der Mitglieder intensivieren und die wichtige Arbeit der ACS stärker in die Verbandsinhalte aufnehmen.

Frage 9: Kennen und nutzen Sie die Allianz für Cybersicherheit?



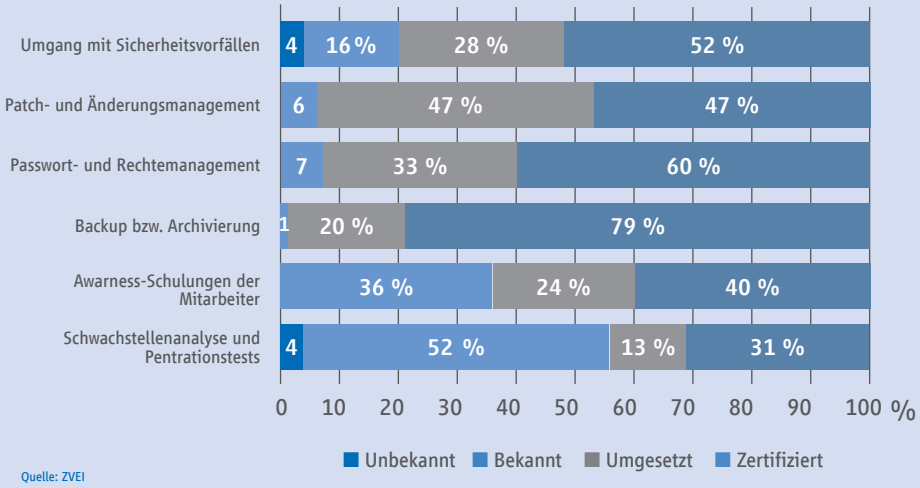
Quelle: ZVEI

[2] Weitere Informationen siehe: https://www.allianz-fuer-cybersicherheit.de/ACS/DE/Home/startseite.html

4 Basismaßnahmen

Für die Umfrage wurde eine Gruppe von sechs Basismaßnahmen gebildet, die zur Mindestanforderung der Cybersicherheit gehören. Unternehmen, die sich zum Beispiel nicht um Back-up, Patchmanagement oder Mitarbeiterschulungen kümmern, stehen vor großen Herausforderungen und Risiken. Zur Unternehmensreife gehört, dass man die Maßnahmen auch dokumentiert und gegebenenfalls testet. Vor diesem Hintergrund ist es ermutigend, dass die Branche bei den Basismaßnahmen gut aufgestellt ist. Die Qualität der Dokumentation oder der Trainingsstand hinsichtlich der Notfallreaktion wurde jedoch nicht abgefragt.

Frage 10: Welche Basis-Maßnahmen setzen Sie ein?



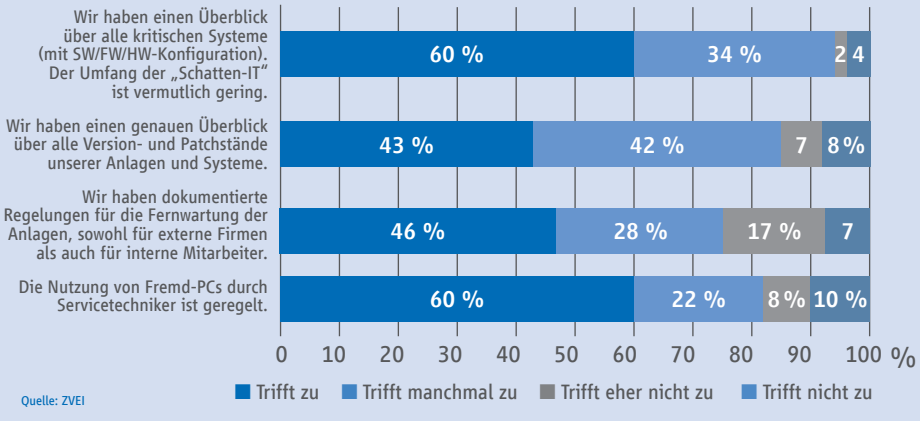
Quelle: ZVEI

Abfrage: Welche der folgenden Aussagen treffen auf Ihre Produktion und Produktions-IT zu?

Im Produktionsbereich kommen oft ältere und sehr heterogene (IT-)Systeme zum Einsatz. Gleichzeitig nimmt auch hier die Vernetzung und Einbindung externer Dienstleistungen zu. Entsprechend wurde speziell für den Produktionsbereich ebenfalls ein Set an Basisanforderung gebildet, um die Organisationreife abzufragen. Sollten diese Maßnahmen nicht berücksichtigt werden, kann es schnell zu Komplikationen im Schadfall kommen. Zusätzlich ist es entscheidend, einen möglichst genauen Überblick über den aktuellen Stand der Hard- und Softwarestände zu haben.

Die Branche setzt die Basismaßnahmen auch im Produktionsbereich mehrheitlich um. Allein die Regelung für Fernwartung und das Handling von externen Mitarbeitern stellt für manche Unternehmen eine Schwierigkeit dar.

Frage 11: Welche der folgenden Aussagen treffen auf Ihre Produktion und Produktions-IT zu?



Quelle: ZVEI

5 Vorfälle und Schäden

5.1 Vorfälle

Die Teilnehmer wurden gebeten, über ein Freifeld mindestens je einen gravierenden Vorfall mit Wirkung im Office- und im Produktionsbereich zu beschreiben. Zur Wahrung der Anonymität kann hier nur eine Clusterung der frei formulierten Inhalte wiedergegeben werden. Folgende Zusammenhänge ergeben sich:

- 37 von 62 Unternehmen waren zum Teil erheblich von Ransomware und Verschlüsselungstrojanern betroffen. Das entspricht 60 Prozent der antwortenden Unternehmen.
- Sechs Prozent der Teilnehmer geben an, dass es einen CEO-Fraud (Versuch) gab.
- Zusätzlich wurden Sonderfälle beschrieben, die keine relevante Häufung hatten. Auffallend ist die Rolle von Identitätsmissbrauch. In sehr unterschiedlichen Varianten kam es dadurch zu Vorfällen im eigenen Netzwerk oder dem von Kunden. Das Spektrum reicht von Kaperung eines Accounts von Mitarbeitern bis zum Versuch, Administratorenrechte zu erlangen.

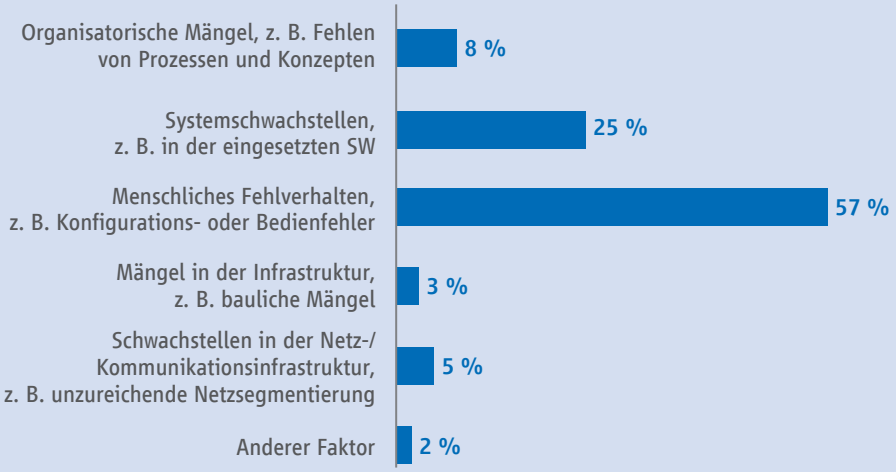
Die Beschreibungen deuten an, dass die Elektroindustrie von gleichen Angriffstrends betroffen ist wie andere Industriesektoren auch. Es lassen sich keine unterschiedlichen Vorgehensweisen oder Angriffstypen feststellen. Dies gilt selbstverständlich nicht für den unbekannten Dunkelbereich, der nicht beschrieben werden konnte.

5.2 Ursachen

Office- und Produktionsbereich

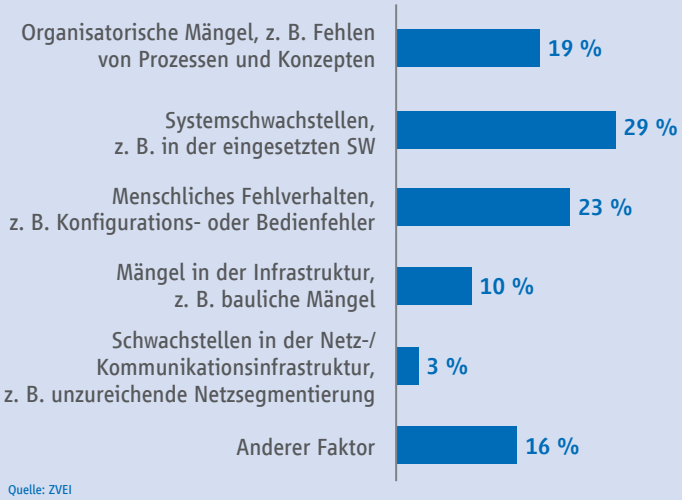
Die möglichen Ursachen für den beschriebenen Sicherheitsvorfall wurden per Multiple Choice erfasst. Im direkten Vergleich zeigen sich interessante Unterschiede im Office- und Produktionsbereich.

Frage 12: Hat einer der folgenden Faktoren zum Eintritt des Sicherheitsvorfalls im Office-Bereich beigetragen?



Quelle: ZVEI

Frage 13: Hat einer der folgenden Faktoren zum Eintritt des Sicherheitsvorfalls im Produktionsbereich beigetragen?



Quelle: ZVEI

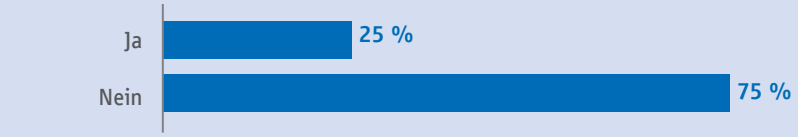
Im Office-Bereich ist der Faktor Mensch üblicherweise die Hauptursache. Der große Anteil von knapp 60 Prozent überrascht wenig. Was die Gründe dafür sind, dass er im Produktionsumfeld auf 22 Prozent zurückgeht, lässt sich nicht definitiv sagen. Eine mögliche Erklärung ist der hohe Anteil an Fachkräften und spezialisierten IT-Systemen in der Produktion, während im klassischen Büro IT-Laien die Systeme bedienen.

6 Strafanzeige und Kooperation mit Behörden

Abfrage: Für den Fall, dass es sich um eine vorsätzliche Straftat handelt, haben Sie bei dem Vorfall Anzeige erstattet?

Weiterhin bleibt die Kooperation mit Behörden eine Herausforderung. Selbst wenn die Unternehmen bereits von einer vorsätzlichen Straftat ausgehen, bringen nur 17 Prozent diesen Vorfall zur Anzeige. Bezeichnenderweise sind dies exakt die gleichen Werte, die der ZVEI in einer kleinen Umfrage 2016 im Fachverband Automation feststellte. Auch vor zwei Jahren meldeten 17 Prozent der Teilnehmer einen Vorfall, 83 Prozent unterließen dies. Anscheinend hat sich in dem Verhältnis der Unternehmen zu den Behörden nichts verändert.

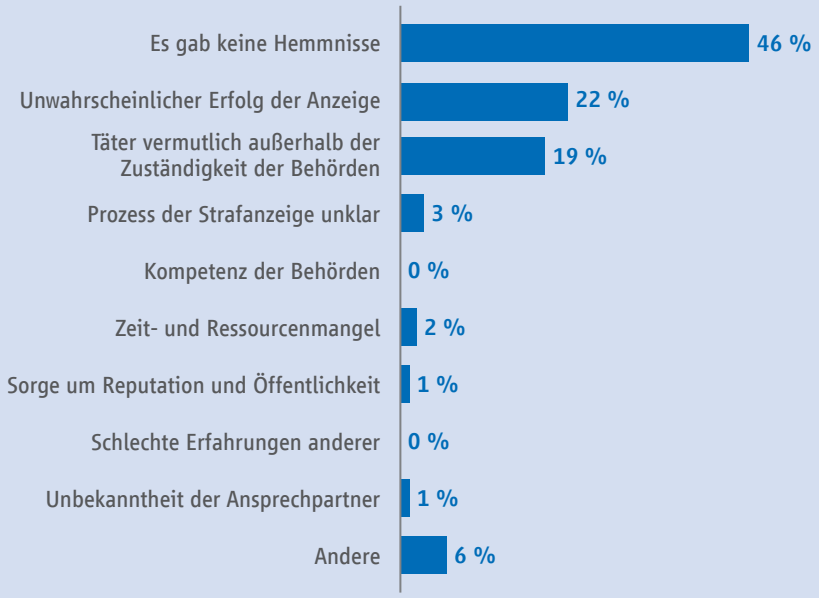
Frage 14: Für den Fall, dass es sich um eine vorsätzliche Straftat handelt, haben Sie bei dem Vorfall Anzeige erstattet?



Quelle: ZVEI

Diejenigen Teilnehmer, die mit „Nein" geantwortet haben, wurden nach dem Grund dafür gefragt. Anders als üblicherweise berichtet, ist es nicht die Angst vor Reputationsschäden (nur 2 % der Teilnehmer geben dies an). Die Hauptfaktoren waren die geringe Aussicht auf Erfolg (21 %) und die fehlenden Zuständigkeiten der Behörden (20 %). Beide Punkte zusammengenommen drücken aus, dass für knapp die Hälfte der Teilnehmer ein mangelndes Vertrauen in die staatliche Handlungsfähigkeit bei Cyberkriminalität der Hinderungsgrund für die Kooperation mit den Behörden ist. Diese Werte sind besorgniserregend und veranlassen den ZVEI, mit den Behörden über bessere und andere Wege der Kooperation zu diskutieren. Ein Schwerpunkt übernimmt hierbei sicherlich die Allianz für Cyber-Sicherheit. Gleichzeitig muss über eine effektivere Bekämpfung der internationalen Cyberkriminalität nachgedacht werden.

Frage 15: Bestanden bei dem Vorfall Hemmnisse, diesen anzuzeigen? Wenn ja, welche?



Quelle: ZVEI

7 Ausblick

Welche ersten Konsequenzen sind aus den Ergebnissen zu ziehen? Als ersten Schritt wird der ZVEI über einen Expertentag am 19. Juni 2018 einen Branchendialog zum Thema „Vertrauenswürdigkeit in der Lieferkette“ initiieren. Die souveräne Bewertung, Integration und Absicherung von eingekaufter Hard- und Software muss leichter möglich sein. Zweitens wird es eine Informations- und Mobilisierungskampagne für die Allianz für Cyber-Sicherheit (ACS) geben. Der ZVEI empfiehlt seinen Mitgliedern, Mitglied in der ACS zu werden, um sich für den Bereich Unternehmenssicherheit in ein effektives Netzwerk einzufügen. Drittens ist zu prüfen, wie ZVEI-Mitglieder darin unterstützt werden können, ein Security-Engineering aufzubauen, um Security by Design tatsächlich umzusetzen. Viertens ist die Anwendungsmöglichkeit internationaler Security-Normen für „Anfänger“ zu überdenken bzw. zu fragen, ob man für die Einführung der Basis-Cybersicherheit alternative Zugänge wählen sollte. Über die Entwicklung eines branchenspezifischen BSI-Grundschutzprofils für die Elektroindustrie wird nachgedacht.

Zusätzlich ist es ein Anliegen des ZVEI, die Weiterentwicklung der Cybersicherheit in der Branche nachzuverfolgen. Geplant ist, einzelne Indikatoren auszuwählen und diese über eine Wiederholung der Umfrage langfristig zu messen. Dies dient auch als Grundlage, die Inhalte und Produkte der Verbandsarbeit entsprechend auszurichten.

Für die Aufstellung der Branche insgesamt wird geprüft, inwiefern CERT- oder Austauschmöglichkeiten für Cybersicherheitsvorfälle – auch in Kooperation mit Partnern – zur Verfügung gestellt werden können.

8 Danksagung

Grundlage für die Erstellung des Sicherheitslagebilds ist die Bereitschaft der ZVEI-Mitgliedsunternehmen, an der Umfrage mitzuwirken. Dies beinhaltet unter anderem tiefergehenden Einblicke in das jeweilige Unternehmen. Wir danken den Mitgliedern für ihr uns entgegengebrachtes Vertrauen und ihre Unterstützung. Ohne dies wäre das Vorhaben nicht möglich gewesen.

Wir hoffen, dass durch dieses Projekt sowohl das Bewusstsein für die Cybersicherheit gestärkt wird als auch konkrete Ansatzpunkte gezeigt werden. Insgesamt soll dies dazu beitragen, dass in der Automation eine positive Sicherheits- und Austauschkultur verfestigt wird. Denn dadurch wird sich die Branche attraktiv für die Zukunft aufstellen.

Über den ZVEI

Der ZVEI - Zentralverband Elektrotechnik- und Elektronikindustrie e. V. vertritt die gemeinsamen Interessen der Elektroindustrie und der zugehörigen Dienstleistungsunternehmen in Deutschland. Rund 1.600 Unternehmen haben sich für die Mitgliedschaft im ZVEI entschieden. Die Branche beschäftigt in Deutschland über 872.000 Arbeitnehmer und weitere 706.000 weltweit.

Der ZVEI repräsentiert eine Branche mit 192 Milliarden Euro Umsatz im Jahr 2017. Etwa 40 Prozent davon entfallen auf neuartige Produkte und Systeme. Jede dritte Neuerung im Verarbeitenden Gewerbe insgesamt erfährt ihren originären Anstoß aus der 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