Bundesamt
für Sicherheit in der
Informationstechnik

**Branchen-Umfrage**
**Im Bereich Automatisierung**
**Durchgeführt von ZVEI-BSI**

ZVEI:
Die Elektroindustrie

# Allgemeine Informationen zur Institution

## 1. In welcher Rolle sind Sie primär tätig?

- ◯ Komponentenhersteller
- ◯ Systemintegrator
- ◯ Andere: [ ]

## 2. In welchem ZVEI Fachverband sind Sie primär tätig?

- ◯ Automation
- ◯ Batterien
- ◯ Consumer Electronics
- ◯ Electrical Winding & Insulation Systems
- ◯ Electronic Components and Systems
- ◯ Elektro-Haushalt-Großgeräte
- ◯ Elektro-Haushalt-Kleingeräte
- ◯ Elektro-Hauswärmetechnik
- ◯ Elektrobahnen und -fahrzeuge
- ◯ Elektroinstallationssysteme
- ◯ Elektromedizinische Technik
- ◯ Elektroschweißgeräte
- ◯ Elektrowerkzeuge
- ◯ Energietechnik
- ◯ Fahr- und Freileitungsbau
- ◯ Kabel und isolierte Drähte
- ◯ Licht
- ◯ Satellit und Kabel
- ◯ Sicherheit
- ◯ Starkstromkondensatoren
- ◯ Transformatoren und Stromversorgung
- ◯ Sonstige

## 3. Wie viele Mitarbeiter beschäftigt Ihr Unternehmen?

- ◯ bis 10 Mitarbeiter
- ◯ bis 50 Mitarbeiter
- ◯ bis 250 Mitarbeiter
- ◯ bis 1.000 Mitarbeiter
- ◯ bis 1.500 Mitarbeiter
- ◯ bis 2.000 Mitarbeiter
- ◯ bis 5.000 Mitarbeiter
- ◯ über 5.000 Mitarbeiter

## 4. Gibt es einen IT-Leiter in Ihrem Unternehmen?

◯ Ja ◯ Nein ◯ Unbekannt

## 5. Gibt es einen Hauptverantwortlichen für die IT-Sicherheit in Ihrem Unternehmen?

◯ Ja ◯ Nein ◯ Unbekannt

## 6. Wird Ihre IT durch einen Dienstleister verwaltet?

- ◯ Ja, Hardware inhouse, Betrieb extern
- ◯ Ja, Hardware und Betrieb extern
- ◯ Nein
- ◯ Unbekannt

## 7. Wird die IT-Sicherheit durch einen Dienstleister verantwortet?

- ◯ Ja, Hardware inhouse, Betrieb extern
- ◯ Ja, Hardware und Betrieb extern
- ◯ Ja, nur überprüft
- ◯ Nein
- ◯ Unbekannt

# Schwerpunkt: Awareness für Cybersicherheit im TOP Management

**8. Cybersicherheit ist ein TOP-Thema in der Geschäftsführung bzw. der Leitungsebene.**

◯ trifft zu ◯ trifft zum Teil zu ◯ trifft eher nicht zu

◯ trifft nicht zu

---

**9. Die Geschäftsführung nimmt Lageberichte zur IT- und Cybersicherheit der Behörden und Security-Community aktiv auf.**

◯ trifft zu ◯ trifft zum Teil zu ◯ trifft eher nicht zu

◯ trifft nicht zu

---

**10. Kennen Sie die überarbeitete Version des BSI Grundschutzes?**

◯ Ja ◯ Nein ◯ Unbekannt

# Fragen zum aktuellen Thema Cloud

## 11. Nutzen Sie Cloud-Dienste?

◯ Ja ◯ Nein ◯ Geplant

---

## 12. Welche Cloud Strategie wird umgesetzt?

**Hinweis:** Diese Frage muss **nicht** beantwortet werden wenn Sie bei Frage 11: "Nutzen Sie Cloud-Dienste?" die Antwort "Nein" angekreuzt haben.

◯ Harware inhouse bereitgestellt, System extern betrieben

◯ Hardware und System extern bereitgestellt und betrieben

◯ Hardware und System intern bereitgestellt und betrieben

---

## 13. Für welche Unternehmensebene setzen Sie Cloud ein?

**Hinweis:** Diese Frage muss **nicht** beantwortet werden wenn Sie bei Frage 11: "Nutzen Sie Cloud-Dienste?" die Antwort "Nein" angekreuzt haben.

◯ ERP-Ebene

◯ Betriebsplanungsebene

◯ Steuerungsebene

◯ Feld- und Komponentenebene

## 14. Waren Security-Aspekte ein Grund, weshalb Sie externe Cloud-Dienste verwenden?

- ◯ Ja, aus Gründen des Security Managements und der Verfügbarkeit
- ◯ Ja, aus anderen Security Gründen
- ◯ Nein, Security war kein ausschlaggebender Grund
- ◯ Wir verwenden keine externen Cloud-Dienste

## 15. Hatten die Änderungen zum Abkommen zu Safe Harbor und Privacy Shield Konsequenzen für die Verwendung externer Cloud-Dienste?

- ◯ Ja, Wechsel des Anbieters
- ◯ Ja, Änderung der Service- und/oder Vertragsbestimmungen
- ◯ Keine Auswirkungen

## 16. Welche der folgenden Aussagen treffen auf Ihren Cloud-Anbieter bzw. Ihr Unternehmen zu?

| | trifft nicht zu | trifft eher nicht zu | trifft manchmal zu | trifft zu |
|---|---|---|---|---|
| Der Cloud-Anbieter besitzt ein definiertes Vorhersagemodell für alle IT-Prozesse (z.B. nach ITIL oder COBIT) | ◯ | ◯ | ◯ | ◯ |
| Der Cloud-Anbieter hat ein ISMS implementiert ( z.B. nach IT-Grundschutz, ISO 27001) | ◯ | ◯ | ◯ | ◯ |
| Der Cloud-Anbieter ist zertifiziert nach einem der folgenden Standards:<br>ISO27001 native<br>ISO27001 auf der Basis von IT-Grundschutz<br>sonstige | ◯ | ◯ | ◯ | ◯ |
| Wir hatten die Möglichkeit, Sicherheitsanforderungen in die SLAs mit dem Cloud-Anbieter einzubeziehen | ◯ | ◯ | ◯ | ◯ |

## 17. Plant Ihr Unternehmen eine Veränderung des Budgets für IT-Sicherheit in den nächsten 12-18 Monaten?

- ◯ Budget erhöhen
- ◯ Budget bleibt gleich
- ◯ Budget sinkt
- ◯ Nicht absehbar

## 18. Wenn Sie Investitionen in IT-Sicherheit vornehmen würden, in welche Bereiche würden Sie primär investieren?

- ◯ in Technik (HW + SW)
- ◯ in Prozesse
- ◯ in Zertifizierung
- ◯ in Neuanstellungen und/oder Schulungen

## 19. Wenn Sie Investitionen in IT-Sicherheit vornehmen wollten, worin sähen Sie die größten Hindernisse?

- ◯ Transparenz des Marktes
- ◯ Qualität der Anbieter und/oder Produkte
- ◯ Inkompatibilität der Lösungen mit bestehenden Systemen
- ◯ Prinzip "Never touch a running system"
- ◯ Budgetbewilligung durch Management
- ◯ Fehlende Produkte und Lösungen für meine Problemstellung und Anliegen
- ◯ Fehlendes Personal bzw. Qualifizierung

# Fragen zum Thema Versicherung

## 20. Setzen Sie eine Versicherung für IT-Sicherheit ein?

◯ Ja ◯ Nein ◯ Unbekannt

---

## 21. War eine Risikoanalyse für IT-Sicherheit Ihres Unternehmens Voraussetzung für das Abschließen der Versicherung?

**Hinweis:** Diese Frage muss nur beantwortet werden wenn Sie bei Frage 20: "Setzen Sie eine Versicherung für IT-Sich..." die Antwort "Ja" angekreuzt haben.

◯ Ja ◯ Nein ◯ Unbekannt

◯ andere Voraussetzungen: _____

---

## 22. War eine Zertifizierung für IT-Sicherheit Ihres Unternehmens Voraussetzung für das Abschließen der Versicherung?

**Hinweis:** Diese Frage muss nur beantwortet werden wenn Sie bei Frage 20: "Setzen Sie eine Versicherung für IT-Sich..." die Antwort "Ja" angekreuzt haben.

◯ Ja ◯ Nein ◯ Unbekannt

◯ andere Voraussetzungen: _____

## 23. Welche genauen Risiken werden von der Versicherung übernommen?

# Fragen zum Thema Vertrauenswürdigkeit

**24. Ist das Thema Vertrauenswürdigkeit (Gewährleistung der Integrität der Daten und Systeme) von Drittprodukten und -lösungen relevant für den Einkauf bzw. Ihr Supply Chain Management?**

◯ Ja ◯ Nein ◯ Unbekannt

---

**25. Über welche Optionen setzen Sie das Thema "Vertrauenswürdigkeit" (z.B. Gewährleistung der Integrität bei Drittprodukten) gegenüber Dritten um?**

- ☐ Vertragsrecht und andere Rechtsmittel
- ☐ Bestimmungen in Einkaufsrichtlinien
- ☐ Prüfung, ob nach Normen und Standards gehandelt wurde
- ☐ Prüfung der Herstellererklärungen
- ☐ Zertifikate
- ☐ Gütesiegel
- ☐ eigene Prüfungen der Produkte und/oder Unternehmung
- ☐ ist kein Thema gegenüber Dritten und Zulieferern
- ☐ Andere

# Fragen zum Thema Risikoanalyse

## 26. Für welche Bereiche Ihres Unternehmens wurde eine Risikoanalyse durchgeführt?

- [ ] Gesamtes Unternehmen mit allen Bereichen
- [ ] Office IT
- [ ] Produktions IT
- [ ] Forschung und Entwicklung
- [ ] Es wurde keine Risikoanalyse durchgeführt

---

## 27. Welche Methode wurde für die Risikoanalayse verwendet?

- ◯ Besichtigungsanalyse
- ◯ Dokumentenanalyse
- ◯ Organisationsanalyse
- ◯ STRIDE
- ◯ DREAD
- ◯ Andere [ ]

## 28. Was waren die größten Hindernisse mit der Risikoanalyse zu beginnen?

- [ ] Unkenntnis der Ansätze und Methoden
- [ ] keine existierende Dokumentenlage
- [ ] fehlende Mitarbeiterkapazitäten
- [ ] fehlende Beratungskompetenzen im Vorfeld
- [ ] schwierige Abstimmung mit Kollegen und Abteilungen
- [ ] keine großen Probleme
- [ ] Andere...

## 29. Allgemeine Kommentare zum Abschnitt der Umfrage

Sind noch andere Inhalte aus Ihrer Sicht relevant, die nicht abgefragt wurden?

# Fokus Office & Office-IT Standards

## 30. Einsatz von IT-Sicherheitsstandards

Welche der folgenden allgemeinen Standards wenden Sie an, und nach welchen Standards ist Ihr Unternehmen ggf. zertifiziert?

| | Unbekannt | Bekannt | Umgesetz | Zertifiziert |
|---|---|---|---|---|
| ISO/IEC 27001 (Informationssicherheit) | ◯ | ◯ | ◯ | ◯ |
| BSI IT-Grundschutz alte Version (Informationssicherheit) | ◯ | ◯ | ◯ | ◯ |
| BSI IT-Grundschutz überarbeitete Version (Informationssicherheit) | ◯ | ◯ | ◯ | ◯ |
| ISO/IEC 22301 (Business Continuity Management) | ◯ | ◯ | ◯ | ◯ |
| ITIL (IT-Prozesse) | ◯ | ◯ | ◯ | ◯ |
| Cobit (IT-Prozesse) | ◯ | ◯ | ◯ | ◯ |
| Common Criteria (Produkte) | ◯ | ◯ | ◯ | ◯ |

## 31. Einsatz von IT-Sicherheitsstandards

Orientieren Sie sich an anderen Security-Standards im Office-Bereich?

# Fokus Produktion & Produktion-IT Standards

## 32. Einsatz von Sicherheitsstandards in der Produktion

Welche der folgenden allgemeinen Standards wenden Sie an, und nach welchen Standards ist Ihr Unternehmen ggf. zertifiziert?

| | Unbekannt | Bekannt | Umgesetz | Zertifiziert |
|---|---|---|---|---|
| VDI/VDE 2182 | ◯ | ◯ | ◯ | ◯ |
| IEC 62443 | ◯ | ◯ | ◯ | ◯ |
| ISO/IEC 27009/27019 | ◯ | ◯ | ◯ | ◯ |

## 33. Einsatz von Sicherheitsstandards in der Produktion

Orientieren Sie sich an anderen Security-Standards für das Produktionsumfeld?

# Umsetzungsstand organisatorischer Maßnahmen

## 34. Feststellung organisatorischer bzw. operativer Schwachstellen

Welche der folgenden Prozesse haben Sie in Ihrem Unternehmen für die Office IT umgesetzt oder dokumentiert?

| | Unbekannt | Bekannt aber nicht umgesetzt | Umgesetzt | Umgesetzt und Dokumentiert |
|---|---|---|---|---|
| Umgang mit Sicherheitsvorfällen | ◯ | ◯ | ◯ | ◯ |
| Patch- und Änderungsmanagement | ◯ | ◯ | ◯ | ◯ |
| Passwort- und Rechtemanagement | ◯ | ◯ | ◯ | ◯ |
| Backup bzw. Archivierung | ◯ | ◯ | ◯ | ◯ |
| Awarness-Schulungen der Mitarbeiter | ◯ | ◯ | ◯ | ◯ |
| Schwachstellenanalyse und Pentrationstests | ◯ | ◯ | ◯ | ◯ |

## 35. Welche der folgenden Aussagen treffen auf Ihre Produktion und Produktions-IT zu?

| | trifft zu | trifft manchmal zu | trifft eher nicht zu | trifft nicht zu |
|---|---|---|---|---|
| Wir haben einen Überblick über alle kritischen Systeme (mit SW/FW/HW- Konfiguration). Der Umfang der "Schatten-IT" ist vermutlich gering. | ◯ | ◯ | ◯ | ◯ |
| Wir haben einen genauen Überblick über alle Version- und Patchstände unserer Anlagen und Systeme. | ◯ | ◯ | ◯ | ◯ |
| Wir haben dokumentierte Regelungen für die Fernwartung der Anlagen, sowohl für externe Firmen als auch für interne Mitarbeiter. | ◯ | ◯ | ◯ | ◯ |
| Die Nutzung von Fremd-PCs durch Servicetechniker ist geregelt. | ◯ | ◯ | ◯ | ◯ |

# Umsetzungsstand technischer Maßnahmen

## 36. Eingesetzte Sicherheitstechnologien

Welche der folgenden technischen Sicherheitsmaßnahmen sind in Ihrem Unternehmen im Einsatz?

| | technisch vor Ort nicht zu realisieren | nicht geplant oder umgesetzt | geplant | umgesetzt |
|---|---|---|---|---|
| Sicherheitsgateways | ◯ | ◯ | ◯ | ◯ |
| Segmentierung von Netzen (physisch) | ◯ | ◯ | ◯ | ◯ |
| Segmentierung von Netzen (logisch) | ◯ | ◯ | ◯ | ◯ |
| SPAM-Abwehr und Content Filtering | ◯ | ◯ | ◯ | ◯ |
| Network Acess Control (NAC) | ◯ | ◯ | ◯ | ◯ |
| Administration von privilegierten Benutzern | ◯ | ◯ | ◯ | ◯ |
| Notstromversorung (USV) und Netzersatzanlage | ◯ | ◯ | ◯ | ◯ |
| VPN | ◯ | ◯ | ◯ | ◯ |
| Abwehr von Schadprogrammen | ◯ | ◯ | ◯ | ◯ |
| Verschlüsselung der Datenträger z.B. Festplattenverschlüsselung (CM) | ◯ | ◯ | ◯ | ◯ |
| Einsatz gehärteter Betriebssysteme und Anwendungen | ◯ | ◯ | ◯ | ◯ |
| Verschlüsselung der Kommunikation z.B. E-Mail, Telephon | ◯ | ◯ | ◯ | ◯ |
| Absicherung mobiler Endgeräte | ◯ | ◯ | ◯ | ◯ |
| Alle kritischen Systeme sind redundant ausgelegt. | ◯ | ◯ | ◯ | ◯ |

# Erkennung von Angriffen

**37. Welche Maßnahmen haben Sie etabliert, um eine Kompromittierung der Produktionsnetze zu detektieren?**

- ◯ Keine
- ◯ Logdatenanalyse
- ◯ Anomalieerkennung
- ◯ Intrusion-Detektion/ Prävention-Systeme (IDS/IPS)
- ◯ Security-Information und Event-Management (SIEM)
- ◯ Andere: [ ]

# Security-Engineering

## 38. Einfach-Auswahlfrage

- ◯ kein Security-Engineering vorhanden
- ◯ Einführung für einzelne Produkte/Lösungen geplant
- ◯ Security-Engineering für einzelne Produkte/Lösungen vorhanden
- ◯ Security-Engineering für nahezu alle Produkte/Lösungen vorhanden
- ◯ Wir haben andere Prozesse in der Entwicklung geplant/umgesetzt

[ ]

# Netzwerk zum Austausch über Cybersicherheit und Vorfälle

## 39. Allianz für Cybersicherheit

| | unbekannt | bekannt | Mitglied | nutzen Inhalte aktiv |
|---|---|---|---|---|
| Kennen und nutzen Sie die Allianz für Cybersicherheit? | ◯ | ◯ | ◯ | ◯ |

## 40. Andere Netzwerke

Nutzen Sie andere Netzwerke für den Informationsaustausch?

## 41. Fokus andere Netzwerke

Für welchen Bereich nutzen Sie Informationsnetzwerke?

◯ nutzen kein Netzwerk ◯ Unternehmenssicherheit

◯ Produktsicherheit

## 42. Allgemeine Kommentare zum Abschnitt der Umfrage

Sind noch andere Inhalte aus Ihrer Sicht relevant, die nicht abgefragt wurden?

# Denken Sie an gravierende Vorfälle in den letzten zwei Jahren (erfragt werden maximal vier Beispiele)

**43. Wie hoch schätzen Sie die Schadenshöhe insgesamt in den letzten beiden Kalenderjahren (laufend 2017 und 2016) für alle erfassten und vermuteten Vorfälle?**

Kosten für Entdeckung, Reaktion, Behebung, Wiederherstellung, Nachverfolgung und Versicherung

# Beschreinung Vorfall Office-IT

**44. Bitte beschreiben Sie einen gravierenden Vorfall mit Wirkung innerhalb der bzw. bezogen auf die Office-IT.**

(Es geht um den Wirkungsort des Vorfalls und nicht um den Eintrittsvektor des Vorfalls)

## 45. Was war die Ursache für den Vorfall?

Mehrfache Nennungen sind möglich.

- [ ] Schadprogramme (Malware)
- [ ] Hacking oder Manipulation (Angriff auf Server / Dienste)
- [ ] Social Engineering (nicht technisch)
- [ ] Missbrauch (Innentäter)
- [ ] physischer Angriff
- [ ] technisches Versagen
- [ ] höhere Gewalt
- [ ] Verhinderung von Diensten (DDOS- Attacken)
- [ ] Identitätsmissbrauch
- [ ] Abhängigkeit von Dienstleistern bzw. Hersteller
- [ ] kombinierter Angriff
- [ ] andere Ursache

## 46. Hat einer der folgenden Faktoren zusätzlich zu den oben genannten Aspekten zum Eintritt des Sicherheitsvorfalls beigetragen?

- [ ] I. Organisatorische Mängel, z. B. Fehlen von Prozessen und Konzepten
- [ ] II. Systemschwachstellen, z. B. in der eingesetzten SW
- [ ] III. Menschliches Fehlverhalten, z. B. Konfigurations- oder Bedienfehler
- [ ] IV. Mängel in der Infrastruktur, z. B. bauliche Mängel
- [ ] V. Schwachstellen in der Netz-/Kommunikationsinfrastruktur, z. B. unzureichende Netzsegmentierung
- [ ] Anderer Faktor

## 47. Was ist die Dauer zwischen Eintreten des Vorfalls und der Erkennung/Meldung des Vorfalls?

- ◯ innerhalb von Sekunden
- ◯ innerhalb von Minuten
- ◯ innerhalb von Stunden
- ◯ innerhalb einer Woche
- ◯ innerhalb eines Monats
- ◯ mehrere Monate
- ◯ innerhalb eines Jahres
- ◯ länger als ein Jahr
- ◯ Dauer unbekannt
- ◯ haben keine Möglichkeit, die Dauer festzustellen

# Auswirkungen Vorfall Office-IT

## 48. Welche Art von Schäden sind bei dem Sicherheitsvorfall entstanden?

- [ ] Imageschaden
- [ ] Finanzieller Schaden durch Ausfall IT-gestützter Geschäftsprozesse
- [ ] Finanzieller Schaden durch Verletzung vertraglicher Vereinbarungen
- [ ] Datenverlust (Verfügbarkeit)
- [ ] Verlust von sensitiven Daten (Vertraulichkeit)
- [ ] Erpressung bzw. Erpressungsversuch
- [ ] Know-How-Abfluss?
- [ ] Kein Schaden entstanden
- [ ] Anderer Schaden

**49. Wie schwerwiegend war der eingetretene Schaden für Ihr Unternehmen?**

- ◯ kein Schaden entstanden
- ◯ unbedeutend
- ◯ begrenzt
- ◯ erheblich
- ◯ schwerwiegend
- ◯ katastrophal / existenzbedrohend

---

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

◯ Ja ◯ Nein

## 51. Bestanden bei dem Vorfall Hemmnisse, diesen anzuzeigen? Wenn ja, welche?

- [ ] Es gab keine Hemmnisse
- [ ] unwahrscheinlicher Erfolg der Anzeige
- [ ] Täter vermutlich außerhalb der Zuständigkeit der Behörden
- [ ] Prozess der Strafanzeige unklar
- [ ] Kompetenz der Behörden
- [ ] Zeit- und Ressourcenmangel
- [ ] Sorge um Reputation und Öffentlichkeit
- [ ] schlechte Erfahrungen anderer
- [ ] Unbekanntheit der Ansprechpartner
- [ ] Andere:

## 52. Welche Lessons Learned haben Sie mitgenommen? Welche Vorkehrungen treffen Sie für die Zukunft?

# Produktion-IT Vorfall 2

**53. Bitte beschreiben Sie einen gravierenden Vorfall mit Wirkung innerhalb der bzw. bezogen auf die Produktion-IT.**

(Es geht um den Wirkungsort des Vorfalls und nicht um den Eintrittsvektor des Vorfalls)

## 54. Was war die Ursache für den Vorfall?

- [ ] Schadprogramme (Malware)
- [ ] Hacking oder Manipulation (Angriff auf Server / Dienste)
- [ ] Social Engineering (nicht technisch)
- [ ] Missbrauch (Innentäter)
- [ ] physischer Angriff
- [ ] technisches Versagen
- [ ] höhere Gewalt
- [ ] Verhinderung von Diensten (DDOS- Attacken)
- [ ] Identitätsmissbrauch
- [ ] Abhängigkeit von Dienstleistern bzw. Hersteller
- [ ] kombinierter Angriff
- [ ] Andere Ursache

## 55. Hat einer der folgenden Faktoren zusätzlich zu den oben genannten Aspekten zum Eintritt des Sicherheitsvorfalls beigetragen?

- [ ] I. Organisatorische Mängel, z. B. Fehlen von Prozessen und Konzepten
- [ ] II. Systemschwachstellen, z. B. in der eingesetzten SW
- [ ] III. Menschliches Fehlverhalten, z.B. Konfigurations- oder Bedienfehler
- [ ] IV. Mängel in der Infrastruktur, z. B. bauliche Mängel
- [ ] V. Schwachstellen in der Netz-/Kommunikationsinfrastruktur, z. B. unzureichende Netzsegmentierung
- [ ] Anderer Faktor

## 56. Was ist die Dauer zwischen Eintreten des Vorfalls und der Erkennung/Meldung des Vorfalls?

- ◯ innerhalb von Sekunden
- ◯ innerhalb von Minuten
- ◯ innerhalb von Stunden
- ◯ innerhalb einer Woche
- ◯ innerhalb eines Monats
- ◯ mehrere Monate
- ◯ innerhalb eines Jahres
- ◯ länger als ein Jahr
- ◯ Dauer unbekannt
- ◯ haben keine Möglichkeit, die Dauer festzustellen

# Auswirkungen Vorfall Produktion-IT

## 57. Welche Art von Schäden sind bei dem Sicherheitsvorfall entstanden?

- [ ] Imageschaden
- [ ] finanzieller Schaden durch Ausfall IT-gestützter Geschäftsprozesse
- [ ] finanzieller Schaden durch Verletzung vertraglicher Vereinbarungen
- [ ] Datenverlust (Verfügbarkeit)
- [ ] Verlust von sensitiven Daten (Vertraulichkeit)
- [ ] Erpressung bzw. Erpressungsversuch
- [ ] Know-How-Abfluss?
- [ ] kein Schaden entstanden
- [ ] Anderer Schaden

**58. Wie schwerwiegend war der eingetretene Schaden für Ihr Unternehmen?**

- ◯ kein Schaden entstanden
- ◯ unbedeutend
- ◯ begrenzt
- ◯ erheblich
- ◯ schwerwiegend
- ◯ katastrophal / existenzbedrohend

---

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

◯ Ja ◯ Nein

## 60. Bestanden bei dem Vorfall Hemmnisse, diesen anzuzeigen? Wenn ja, welche?

- [ ] Es gab keine Hemmnisse
- [ ] Unwahrscheinlicher Erfolg der Anzeige
- [ ] Täter vermutlich außerhalb der Zuständigkeit der Behörden
- [ ] Prozess der Strafanzeige unklar
- [ ] Kompetenz der Behörden
- [ ] Zeit- und Ressourcenmangel
- [ ] Sorge um Reputation und Öffentlichkeit
- [ ] schlechte Erfahrungen anderer
- [ ] unbekanntheit der Ansprechpartner
- [ ] Andere:

## 61. Können Sie noch weitere gravierende Vorfälle nennen?

◯ Ja ◯ Nein

## 62. Bitte beschreiben Sie einen gravierenden Vorfall.

**Hinweis:** Diese Frage muss nur beantwortet werden wenn Sie bei Frage 61: "Können Sie noch weitere gravierende Vorf..." die Antwort "Ja" angekreuzt haben.

Textfeld

# Allgemeine Kommentare

**63. Möchten Sie noch Anmerkungen zu der Umfrage für uns hinterlassen?**

Bundesamt
für Sicherheit in der
Informationstechnik

Branchen-Umfrage
Im Bereich Automatisierung
Durchgeführt von ZVEI-BSI

ZVEI:
Die Elektroindustrie

# Ende der Umfrage

## Haben Sie vielen Dank für Ihre Teilnahme!

Nach Abschluss der Umfrage können Sie die Umfrage nicht wieder öffnen. Ihre Antworten können Sie hier ausdrucken. Ein Auswertungsbericht erfolgt zu Beginn 2018.

Ansprechpartner: Lukas Linke (linke@zvei.org)