Bundesamt
für Sicherheit in der
Informationstechnik

Aktuelle Entwicklungen und Initiativen

10. Juli 2019

Stefan Becker
Bundesamt für Sicherheit in der Informationstechnik

Warum Notfallmanagement?

Allianz für Cyber-Sicherheit

Malware war 2018 mit 53 Prozent die **häufigste Form von Cyber-Angriffen** auf deutsche Unternehmen und Institutionen.

In 90 Prozent der Fälle dienten dabei **schädliche Anhänge oder Links in E-Mails als Einfallstor**.

In der **Hälfte der E-Mail-basierten Angriffe** verhinderten **technische Maßnahmen** eine Infektion, in den übrigen Fällen war die vorausgegangene **Sensibilisierung und Schulung der Beschäftigten** der Erfolgsfaktor.

33 Prozent der Unternehmen sind **2018 Opfer von Cyber-Angriffen** geworden. (Großunternehmen 43 Prozent, kleine und mittelständische 26 Prozent)

Rund **87 Prozent** der von Cyber-Sicherheitsvorfällen Betroffenen gaben an, dass es 2018 in der Folge zu **Betriebsstörungen oder -ausfällen** kam.

Hinzu kamen weitere **Kosten**: Aufklärung der Vorfälle und die Wiederherstellung der IT-Systeme (bei 65 Prozent) sowie Reputationsschäden (22 Prozent).

UMFRAGE 2018

Cyber-Sicherheits-Warnungen: Emotet

Allianz für Cyber-Sicherheit

Gefährliche Schadsoftware

- Groß angelegte Spamkampagne mit authentisch aussehenden E-Mails.
- Methoden hochprofessioneller APT-Angriffe adaptiert und automatisiert
- ab November 2018

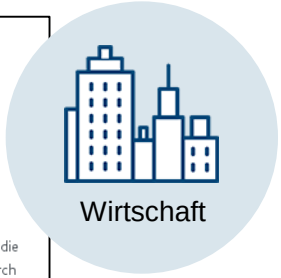
Empfohlene Schutzmaßnahmen:
www.allianz-fuer-cybersicherheit.de/ACS/emotet

Gefährliche Schadsoftware – BSI warnt vor Emotet und empfiehlt Schutzmaßnahmen

Ort Bonn
Datum 05.12.2018

Gefälschte E-Mails im Namen von Kollegen, Geschäftspartnern oder Bekannten - Schadsoftware, die ganze Unternehmensnetzwerke lahm legt: Emotet gilt als eine der gefährlichsten Bedrohungen durch Schadsoftware weltweit und verursacht auch durch das Nachladen weiterer Schadprogramme aktuell hohe Schäden auch in Deutschland. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat in den vergangenen Tagen eine auffällige Häufung an Meldungen zu schwerwiegenden IT-Sicherheitsvorfällen erhalten, die im Zusammenhang mit Emotet stehen. In Einzelfällen ist es bei den Betroffenen durch Ausfälle der kompletten IT-Infrastruktur zu Einschränkungen kritischer Geschäftsprozesse gekommen, die Schäden in Millionenhöhe nach sich ziehen. Daneben sind dem BSI weitere Fälle mit weniger schwerem Verlauf gemeldet worden, bei denen Malware-Analysten des BSI Emotet-Infektionen nachweisen konnten. Emotet wird derzeit weiterhin über groß angelegte Spam-Kampagnen verteilt und stellt daher eine akute Bedrohung für Unternehmen, Behörden und Privatanwender dar. Das BSI hat im Rahmen seines gesetzlichen Auftrags KRITIS-Betreiber, staatliche Einrichtungen in Bund und Ländern sowie Teilnehmer der Allianz für Cyber-Sicherheit heute erneut vor Emotet gewarnt und effektive umfassende Schutzmaßnahmen empfohlen. Angepasst an die Zielgruppen Unternehmen und Privatanwender sind diese auf den Webseiten des BSI abrufbar unter
› https://www.allianz-fuer-cybersicherheit.de/ACS/emotet und › https://www.bsi-fuer-buerger.de/BSIFB/emotet.

Quelle: bsi.bund.de



Bundesamt für Sicherheit in der Informationstechnik

Aktueller IT-Sicherheitsvorfall: Emotet

Allianz für Cyber-Sicherheit

Angriff nicht durch einzelne Maßnahmen abzuwehren. Gestaffelte Verteidigung: Hardware, Software, Mitarbeiter

Security ist Aufgabe jedes Mitarbeiters.
Das Management tritt als Vorbild auf.

Das Problem nicht auf die Mitarbeiter abschieben!
Eine sichere IT-Landschaft ist notwendig.

Selbst nach erfolgreicher Vorfallsbehandlung ist ein erneuter Vorfall nicht zu verhindern.

Quelle: heise.de

Business Continuity Management (BCM)

Teil 1 des Notfallmanagements

Allianz für Cyber-Sicherheit

Jede Institution sollte jederzeit auf Störungen
und Notfälle vorbereitet sein.

Verantwortlichkeiten und Abläufe
sind im Vorfeld zu definieren.

Der richtige Mix aus technischen Maßnahmen und
Sensibilisierung (Schulung, Gamification, Nudging) ist wichtig.

Das korrekte Verhalten sollte regelmäßig
in Übungen trainiert werden.

Detektion

Allianz für Cyber-Sicherheit

Die aktive und anlassbezogene Auswertung von Log-Dateien wir oft empfohlen und selten gemacht.

Monitoring auch für vertrauenswürdige Verbindungen: VPN-Zugang eines Kunden (Supply-Chain-Attack)

IT-Sicherheitstechnik braucht IT-Sicherheitstechniker!

Incident Response

Teil 2 des Notfallmanagements

Allianz für Cyber-Sicherheit

Ruhe bewahren!

Krisenkommunikation kann der Schlüssel sein, um Reputationsschäden zu vermeiden.

Holen sie sich Rat & Unterstützung. Meist kann nur durch professionelle Hilfe eine Bereinigung gesichert werden. Support im Rahmen von Cyber-Versicherungen?

Das korrekte Verhalten sollte regelmäßig in Übungen trainiert werden.

Bundesamt für Sicherheit in der Informationstechnik

Cyber-Resilienz

Allianz für Cyber-Sicherheit

Assume the breach!

Schlüsselkompetenz der Zukunft

Steigerung der Anzahl der Vorfälle &
Qualität der Angriffe nimmt zu

Netzwerke schützen Netzwerke!

Der

Routenplaner

IT-Grundschutz
Informationssicherheit in der Praxis

Allianz für Cyber-Sicherheit

IT-Grundschutz verfolgt einen ganzheitlichen Ansatz.

Infrastrukturelle, organisatorische, personelle und technische Standard-Sicherheitsanforderungen helfen, ein Standard-Sicherheitsniveau aufzubauen, um geschäftsrelevante Informationen zu schützen.

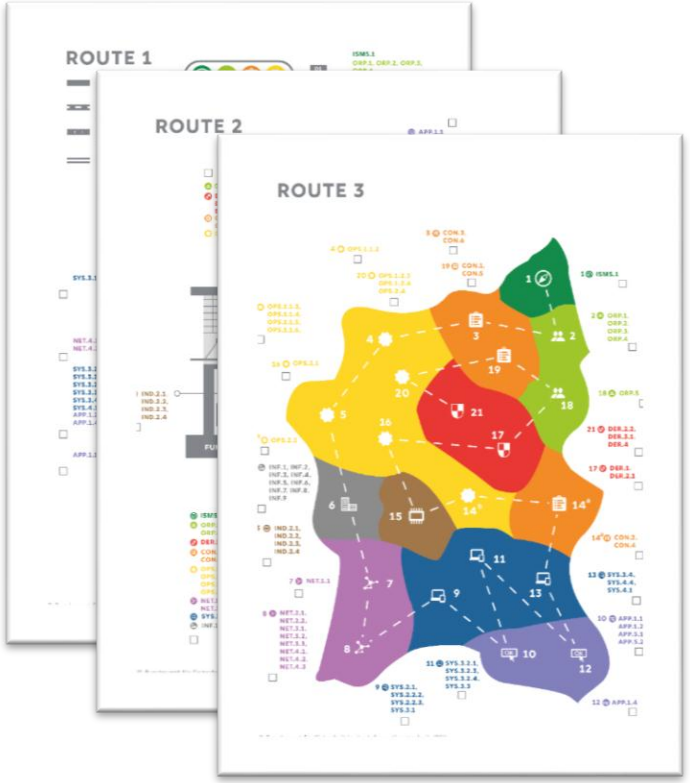
An vielen Stellen werden bereits höherwertige Sicherheitsanforderungen geliefert, die die Basis für sensiblere Bereiche sind.

Bundesamt
für Sicherheit in der
Informationstechnik

Routenplaner „Cyber-Sicherheit für Handwerksbetriebe“

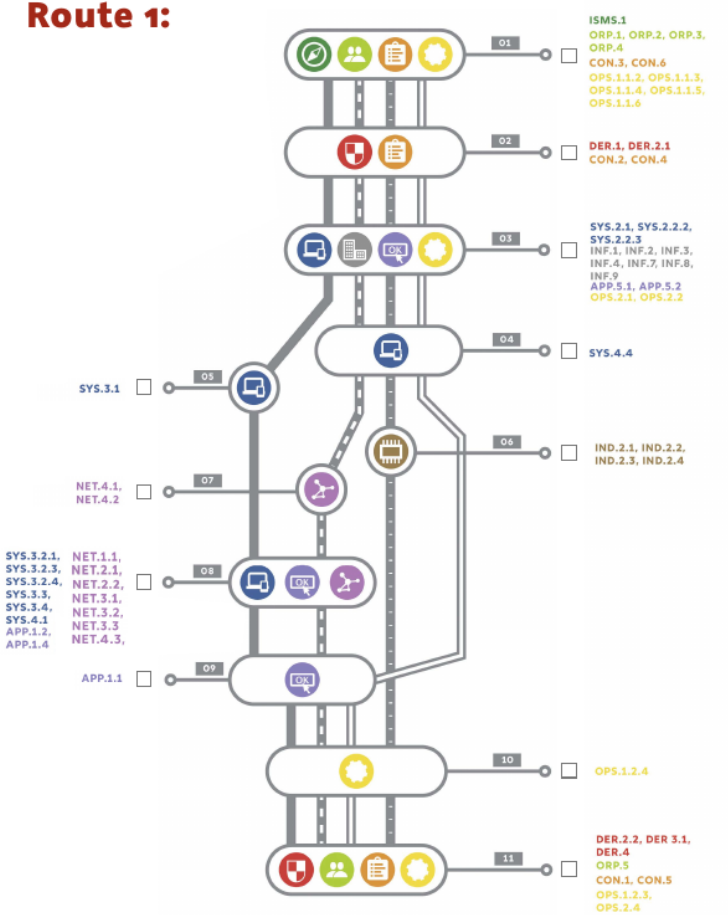
Allianz für Cyber-Sicherheit

- Basiert auf dem IT-Grundschutz-Profil für Handwerksbetriebe
- Zeigt praktische Wege auf, wie kleine und mittelständische Unternehmen das Thema Informationssicherheit zielgerichtet umsetzen können
- Auswahl aus 3 Routen, um den individuellen Sicherheitsprozess nach IT-Grundschutz bedarfsgerecht zu gestalten
- Anschauliche Routenpläne und zielgruppengerechte Arbeitshilfen



Bundesamt für Sicherheit in der Informationstechnik

Route 1:



Erklärung zu den IT-Grundschutzbausteinen siehe Seite 12.

Betrieblich.

IT-unterstützte Abläufe sind in vielen Betrieben nicht mehr wegzudenken – sei es in der Auftragsgewinnung, der Angebotserstellung, Auftragsdurchführung oder Abrechnung.

Mit der Route 1 durchlaufen Sie typische Aufgabenbereiche Ihres Betriebs. Welcher Bereich ist für Ihren Geschäftserfolg besonders relevant? Machen Sie ein Ranking. Starten Sie mit dem wichtigsten Bereich und widmen Sie sich danach den anderen. Egal, mit welchem Weg Sie beginnen: Sie generieren in jedem Fall Synergien. Denn sobald sie einen der vier Wege in dieser Route absolviert haben, sind bereits große Teile der anderen Wege erledigt. Wurden alle der insgesamt elf Stationen angesteuert, haben Sie das vollständige Profil geschafft.

Ihre Wege im Überblick.

Auftragsgewinnung:
Sie durchlaufen die Stationen 1, 2, 3, 5, 8, 9, 10 und 11. Für das vollständige Profil fehlen nur noch die Stationen 4, 6 und 7.

Angebotserstellung:
Mit den Stationen 1, 2, 3, 4, 7, 8, 9, 10 und 11 haben Sie den größten Teil der Route absolviert – das vollständige Profil erreichen Sie über die Stationen 5 und 6.

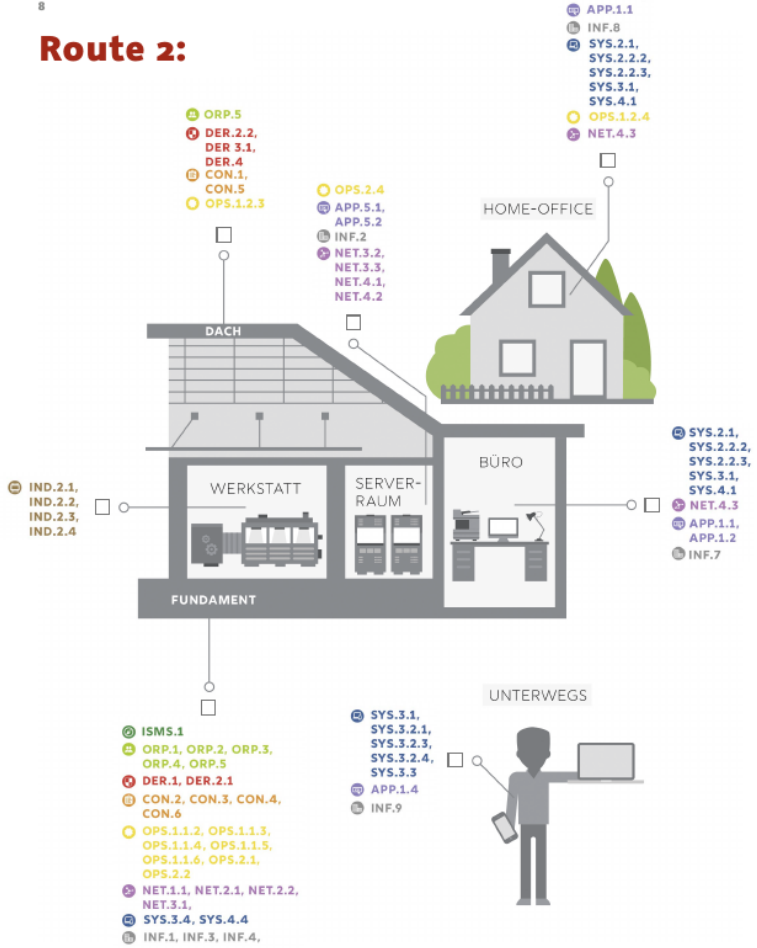
Auftragsdurchführung:
Dieser Weg ist eine Art Schnelldurchgang über die Stationen 1, 2, 3, 4, 6, 10, 11. Vollständig wird das Profil, wenn Sie noch die Stationen 5, 6, 7, 8 und 9 nachlegen.

Abrechnung:
Für Schnellrechner: Wer auf diesem Weg die Stationen 1, 2, 3, 4, 9, 10, 11 zurücklegt, muss für das vollständige Profil nur noch die Stationen 5, 6, 7 und 8 schaffen.

Tipp für die Praxis:
Kleine Ergänzung zur Bedienungshilfe „1, 2, 3 – So wird's gemacht" (S.4): Sie finden in der Abbildung S.6 neben den Bausteinen an den elf Stationen jeweils eine Checkbox. Hier kommt der Haken hin, wenn Sie eine Etappe geschafft haben.

Bundesamt
für Sicherheit in der
Informationstechnik

Route 2:



Räumlich.

Beim Rundgang durch die Betriebsstätte wird eines deutlich: Die Digitalisierung ist im Handwerk angekommen. Am Empfang ein PC, in der Ecke des Büros der Router, in der Werkstatt vielleicht eine IT-unterstützte Maschine, unterwegs ein Smartphone, im Home-Office ein Laptop. Räumen Sie auf und machen Sie Ihre Räume mitsamt IT-System(en) sicher.

Route 2 führt Sie von Raum zu Raum – und auch unterwegs – zu mehr Informationssicherheit im Betrieb. Beginnen Sie dort, wo Sie schon immer einmal Ordnung machen wollten und nehmen Sie sich dann nach und nach die anderen Räume vor. Auf diese Weise erarbeiten Sie sich alle notwendigen Bausteine. Es gibt allerdings eine Bedingung: Fundament und Dach sind Pflicht.

Ihre Räume im Überblick.

Pflichtprogramm zu Beginn: Fundament:
Bloß nicht auf Sand bauen – die hier aufgelisteten Bausteine sind für den gesamten Betrieb wichtig, damit legen Sie eine solide Basis für Ihre Informationssicherheits-Architektur.

Serverraum:
An diesem Ort läuft vieles zusammen – Im Serverraum befindet sich die Hardware, die der Bereitstellung von Diensten und Daten im Betrieb dient.

Büro:
Büro ist nicht gleich Büro, aber jeder Raum der Betriebsstätte, in dem IT-unterstützt Angebote erstellt werden oder die Abrechnung erfolgt, kann als Büroraum im Sinne dieser Route gewertet werden.

Werkstatt:
Gehören Sie zum produzierenden Handwerk? Dann sollten Ihre IT-unterstützten Maschinen sicher sein.

Home-Office:
Home Secure Home – so sollte das Motto lauten, wenn betriebseigene Informationen an einem häuslichen Arbeitsplatz bearbeitet werden.

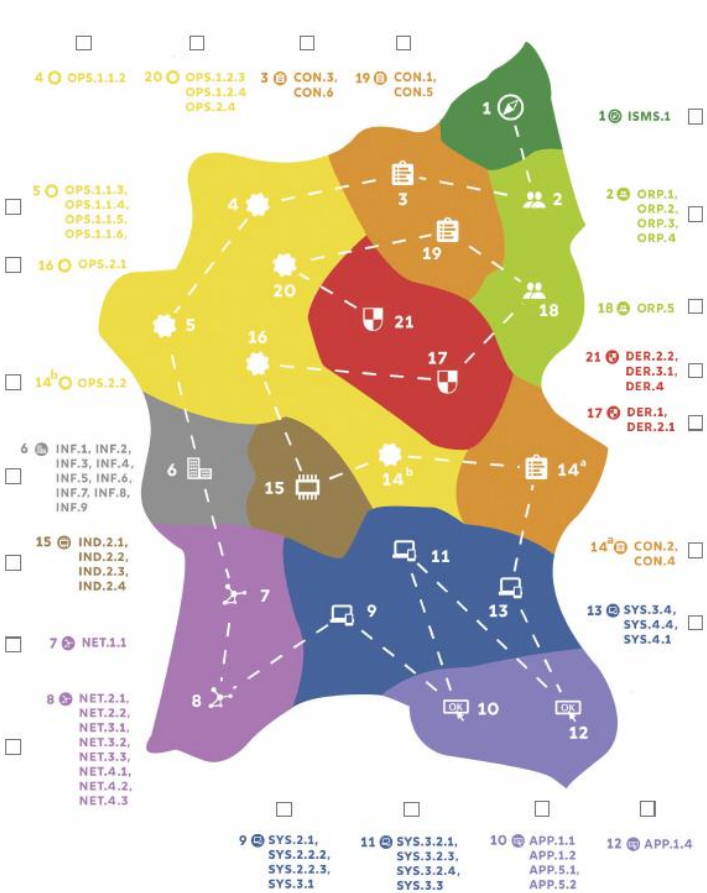
Unterwegs von Raum zu Raum:
Ob auf der Straße, beim Kunden, auf Geschäftsreisen oder zwischendurch mal von zu Hause aus – wechselnde Arbeitsplätze bedeuten unterschiedliche Umgebungen und damit erhöhte Anforderungen an die Informationssicherheit.

Pflichtprogramm zum Schluss: Dach:
Setzen Sie zum Schluss Ihren Räumen die Krone auf.

Tipp für die Praxis:
Kleine Ergänzung zur Bedienungshilfe „1, 2, 3 – So wird's gemacht" (S.4): Bitte beachten Sie insbesondere die Reihenfolge (R1 bis R3) in der Bearbeitung der Bausteine und gehen Sie vom Wesentlichen zum eher Nachrangigen. Und: In die Checkbox kommt ein Haken, wenn Sie diesen Raum erledigt haben.

Bundesamt
für Sicherheit in der
Informationstechnik

Route 3:



Thematisch.

Sie interessieren sich für die zentralen Themen der Informationssicherheit? Und Sie möchten alle Bausteine aus dem „IT-Grundschutz-Profil für Handwerksbetriebe" von Anfang bis Ende systematisch durcharbeiten?

Route 3 orientiert sich deutlich an der IT-Grundschutz-Methode und leitet Sie Schritt für Schritt durch die zehn Schichten unter Beachtung der empfohlenen Umsetzungsreihenfolge R1 bis R3.

ISMS: Grundlage für alle weiteren Aktivitäten im Sicherheitsprozess

ORP: Organisatorische und personelle Sicherheitsaspekte

CON: Konzepte und Vorgehensweisen

OPS: Sicherheitsaspekte des operativen IT-Betriebs

DER: Detektion von Sicherheitsvorfällen und Reaktion bei Vorfällen

APP: Anwendungen und Dienste

SYS: IT-Systeme

IND: Industrielle IT – Produktion

NET: Netzverbindungen und Kommunikation

INF: Aspekte der infrastrukturellen Sicherheit

Ihre Stationen im Überblick.

1. Grundlage für Ihre Informationssicherheit
2. Organisation und Personal
3. Konzeptionelle Grundlagen für Datensicherheit
4. Die eigenständige IT-Administration? (sonst überspringen)
5. Grundlagen für den technischen Betrieb
6. Schaffung einer sicheren Infrastruktur
7. Planvolle Entwicklung und Aufbau eines Netzwerks
8. Sicherung einzelner Netzwerkkomponenten
9. Standard IT – Hardware
10. Standard IT – Software
11. Mobile IT – Hardware
12. Mobile IT – Software
13. Sonstige IT und Peripherie
14. a Aufbauende Konzepte
14. b Aufbauende Konzepte
15. Sichere Produktion
16. Die extern gehostete Website
17. Grundlagen der Detektion und Reaktion
18. Informationssicherheit und Rechtliches
19. Verschlüsselung und Software-Entwicklung
20. IT-Sicherheit in komplexen Einsatzszenarien
21. Professionelles Cyber-Vorfallmanagement

Tipp für die Praxis:
Kleine Ergänzung zur Bedienungshilfe „1, 2, 3 – So wird's gemacht" (S.4): Nutzen Sie die auf Seite 10 dargestellte Übersicht als Checkliste.

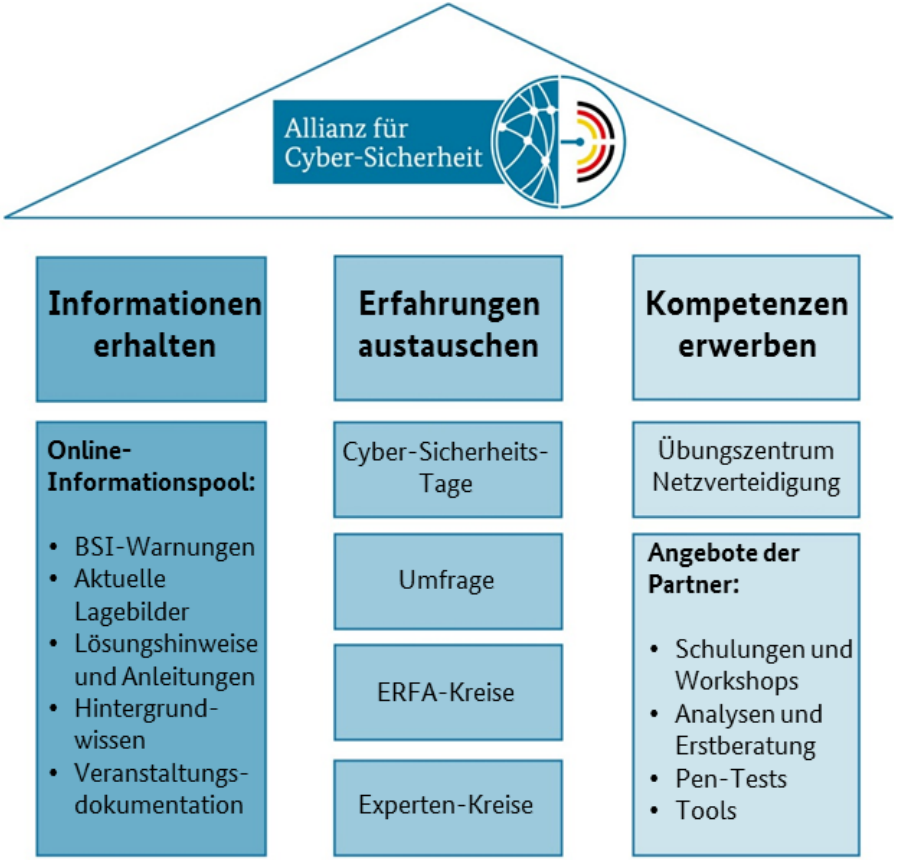
Bundesamt
für Sicherheit in der
Informationstechnik

Die

Allianz für Cyber - Sicherheit

Die Allianz für Cyber-Sicherheit

Allianz für Cyber-Sicherheit



Bundesamt für Sicherheit in der Informationstechnik

Aufgabenspektrum:
Prävention, Detektion und Reaktion

Allianz für Cyber-Sicherheit

Informationen, Empfehlungen und Vorgaben

Beispiele:

- IT-Grundschutz / BSI-Standards
- Technische Richtlinien und Studien
- Lagebericht/ -bild
- Warnungen

Fortbildungen, Vorträge und Demonstrationen

Beispiele:

- Live-Hacking
- Fortbildung „Übungszentrum Netzverteidigung“

Erfahrungsaustausch

Allianz für Cyber-Sicherheit

Cyber-Sicherheits-Tage

29. Cyber-Sicherheits-Tag am 26.09.2019 in Berlin
Thema: **„Netzwerke schützen Netzwerke“**

30. Cyber-Sicherheits-Tag am 26.11.2019 in Stuttgart
Thema: **„Industrial Control System (ICS) Security”**

Kreise (Auszug)

- Erfahrungskreis „Praxisorientierte Awareness“
- Erfahrungskreis „Geheimschutz“

www.allianz-fuer-cybersicherheit.de

Bundesamt für Sicherheit in der Informationstechnik

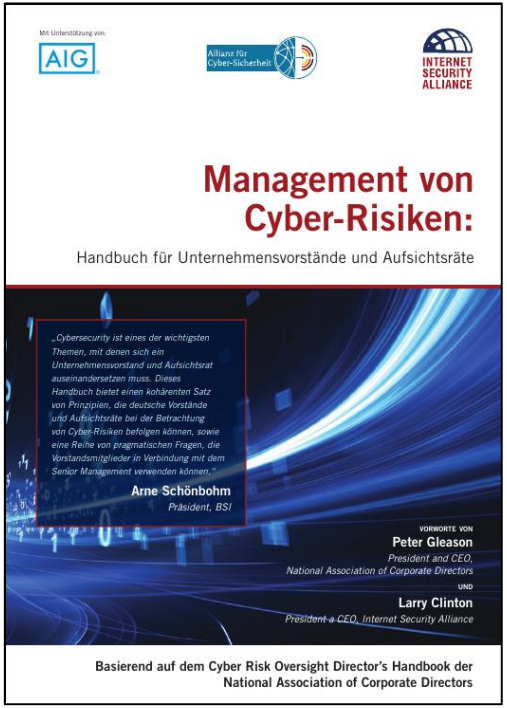
Partner-Angebote (Auszug)

Allianz für Cyber-Sicherheit

Kategorie	Titel	Ort
Simulation	Kaspersky KIPS: Angriff aufs Unternehmensnetzwerk	München
Beratung	Apropos Emotet: Security-Awareness-Standortbestimmung für Unternehmen	*
Seminar	Web Application Security – OWASP Top 10 2017	München
Seminar	Awareness kompakt für Führungskräfte	Berlin
Awareness-Poster	Psychotricks und Phishing-Maschen	*
Workshop (CTF)	KrimiDinner 2.0	Köln

Management von Cyber-Risiken

Handbuch für Unternehmensvorstände und Aufsichtsräte



5 grundlegende Prinzipien für das Management:

1. Cyber-Sicherheit als Thema des unternehmensweiten **Risiko-Managements** verstehen
2. Prinzip 2: **Rechtliche Auswirkungen** von Cyber-Risiken verstehen
3. Prinzip 3: Grundlegende **Cyber-Sicherheits-Expertise** erwerben
4. Prinzip 4: Umsetzung geeigneter **Rahmenbedingungen und Ressourcen** für das Cyber-Risiko-Management sicherstellen
5. Prinzip 5: **Risikobereitschaft** in Abhängigkeit von Geschäftszielen und -strategien definieren

https://www.allianz-fuer-cybersicherheit.de/NACD-Handbuch

Bundesamt für Sicherheit in der Informationstechnik

Allianz für Cyber-Sicherheit

"Amateurs hack systems, professionals hack people.“

- Bruce Schneier

Informationen:

Allianz für Cyber-Sicherheit

Stefan Becker

Kontakt

Geschäftsstelle der Allianz für Cyber-Sicherheit
c/o Bundesamt für Sicherheit in der Informationstechnik (BSI)

Godesberger Allee 185 – 189
53175 Bonn

info@cyber-allianz.de
www.allianz-fuer-cybersicherheit.de
Tel. +49 (0) 228 99 9582 5977
Fax +49 (0) 228 99 109582 6050

Sie finden uns auch in Sozialen Netzwerken.

Twitter

www.twitter.com/CyberAllianz

Xing

www.xing.com/net/allianz-fuer-cybersicherheit

Bundesamt für Sicherheit in der Informationstechnik