Bundesamt
für Sicherheit in der
Informationstechnik

IT-Sicherheit im HomeOffice

Stefan Becker
Bundesamt für Sicherheit in der Informationstechnik

01.07.2021 | 8. GELSEN-NET Security Day

Wie bedroht ist Deutschlands Cyber-Raum?

- Angreifer nutzen **Schadprogramme für cyber-kriminelle Massenangriffe** aber auch für **gezielte Angriffe** auf ausgewählte Opfer.
- In einer neuen Schadprogramm-Welle im **dominiert Emotet die Lage**.
- Rund **117,4 Mio. Variationen von neuen Schadprogrammen** wurden im Berichtszeitraum gesichtet. Das sind durchschnittlich **322.000 pro Tag, in Spitzenwerten 470.000**.
- Knapp **7 Millionen Meldungen zu Schadprogramm-Infektionen** hat das BSI an deutsche Netzbetreiber übermittelt.
- Bei Angriffen auf die Bundesverwaltung wurden rund **35.000 E-Mails mit Schadsoftware pro Monat** abgefangen.
- **24,3 Millionen Patientendatensätze** waren Schätzungen zufolge international frei im Internet zugänglich.
- Cyber-Kriminelle nutzen **COVID-19-Pandemie** für Social-Engineering-Angriffe aus.

Quelle: BSI

Die Auswirkungen der COVID-19-Pandemie

Das „New Normal“

Forcierung der Digitalisierung von Prozessen

Vermehrte Nutzung von Remote-Arbeitsplätzen

Aufbau langfristiger Fähigkeiten zu dislozierten Arbeiten

Höhere Gefährdungslage

Häufig Funktionalität vor Sicherheit

Verändertes Verhalten der Sicherheitsverantwortlichen und der Benutzer

Ausnutzung der Situation durch Social Engineering

→ Positive Aspekte beibehalten und Überführung von Ad-hoc Maßnahmen in einen sicheren Regelbetrieb!

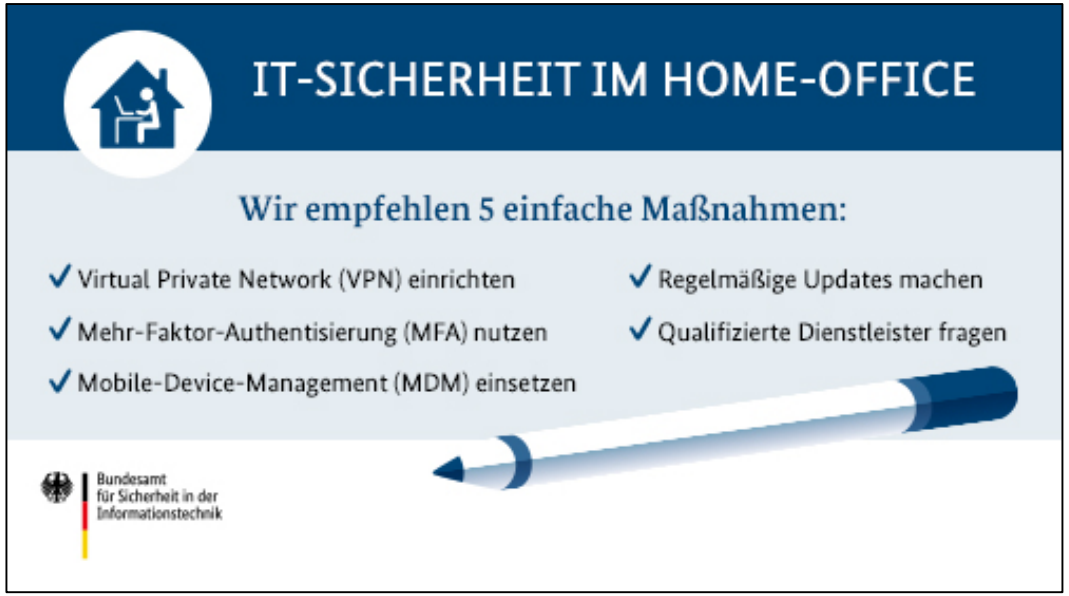
Ziele von Cyber-Angriffen

- **Unternehmen und Institutionen aller Größen und Branchen**. So wurden Automobilhersteller und ihre Zulieferer angegriffen, ebenso wie Flughäfen und Fluggesellschaften.
- **Kleine und mittelständische Unternehmen**, die sich durch Alleinstellungsmerkmale wie zum Beispiel die Produktion spezieller Komponenten im Maschinenbau auszeichnen.
- **Kommunale Verwaltungen, Krankenhäuser und Hochschulen** sind von Ransomware-Angriffen betroffen.

Quelle: BSI

Maßnahmen für IT-Sicherheit im Homeoffice

Allianz für Cyber-Sicherheit



Videokonferenz-Kompetenz

Quelle: Twitter-Account Rihards Kohls

Gesicherte Identität?

Quelle: Focus Online

Unbekannte Teilnehmende?

Bundesamt
für Sicherheit in der
Informationstechnik

IT-sichere Videokonferenzen

- Kompendium Videokonferenzsysteme

https://www.allianz-fuer-cybersicherheit.de/Webs/ACS/DE/Informationen-und-Empfehlungen/Empfehlungen-nach-Angriffszielen/Remote/Videokonferenzsysteme/videokonferenzsysteme_node.html

- BSI-Empfehlung zum IT-sicheren Einsatz von Jitsi Meet

https://www.allianz-fuer-cybersicherheit.de/SharedDocs/Downloads/Webs/ACS/DE/BSI-CS/BSI-CS_143.pdf?__blob=publicationFile&v=4

- Leitfaden für virtuelle Events

https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Veranstaltungen/ECSM/Leitfaden_virtuelles_Event.html?nn=906564

- Virtuelle Versammlungen und Abstimmungen (Community Draft)

https://www.allianz-fuer-cybersicherheit.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Themen/Virtuelle_Versammlungen_Abstimmungen.pdf?__blob=publicationFile&v=1

- Co-Moderationskarten für virtuelle Meetings

https://www.allianz-fuer-cybersicherheit.de/Webs/ACS/DE/Informationen-und-Empfehlungen/Empfehlungen-nach-Angriffszielen/Remote/Home-Office/Co-Moderationskarten/co-moderationskarten-node.html

Bundesamt für Sicherheit in der Informationstechnik

Awareness – Sicherheitsfaktor Mensch

- Sensibilisieren für IT-Sicherheit am Arbeitsplatz
- Regelmäßige Awareness-Übungen
- Kein Risiko – sondern Sicherheitsfaktor Mensch
- Etablierte „Cyber-Sicherheits“-Kultur im Unternehmen

Bundesamt für Sicherheit in der Informationstechnik

Service-Paket für mehr Cyber-Resilienz

Allianz für Cyber-Sicherheit

VERHALTEN BEI IT-NOTFÄLLEN

Ruhe bewahren & IT-Notfall melden
Lieber einmal mehr als einmal zu wenig anrufen!

IT-Notfallrufnummer:

Wer meldet?

Welches IT-System ist betroffen?

Wie haben Sie mit dem IT-System gearbeitet?
Was haben Sie beobachtet?

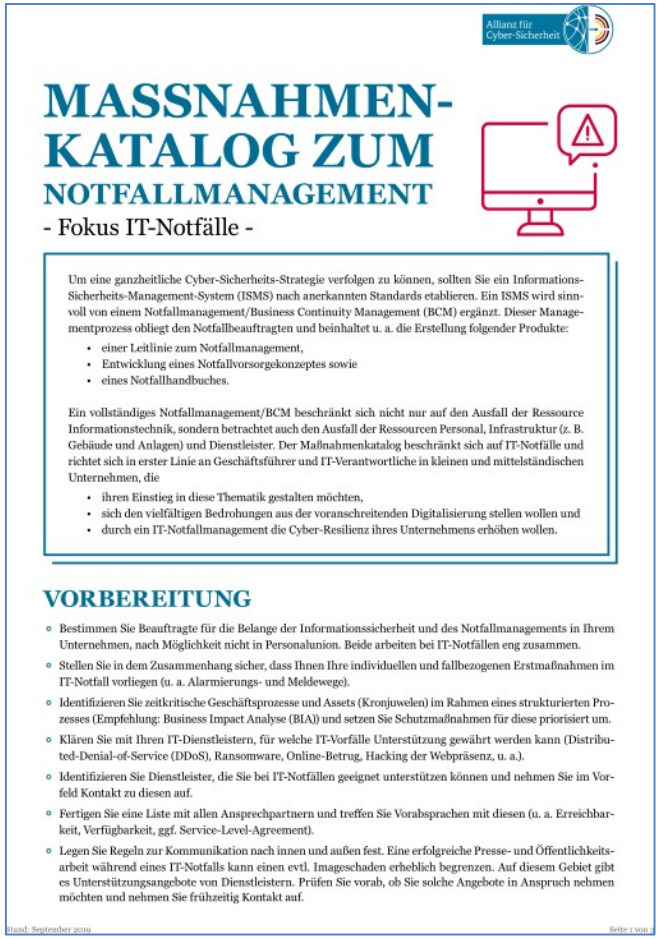
Wann ist das Ereignis eingetreten?

Wo befindet sich das betroffene IT-System?
(Gebäude, Raum, Arbeitsplatz)

Verhaltenshinweise

Weitere Arbeit am IT-System einstellen	Beobachtungen dokumentieren	Maßnahmen nur nach Anweisung einleiten

Herausgeber: Bundesamt für Sicherheit in der Informationstechnik



Allianz für Cyber-Sicherheit

MASSNAHMEN-KATALOG ZUM NOTFALLMANAGEMENT

- Fokus IT-Notfälle -

Um eine ganzheitliche Cyber-Sicherheits-Strategie verfolgen zu können, sollten Sie ein Informations-Sicherheits-Management-System (ISMS) nach anerkannten Standards etablieren. Ein ISMS wird sinnvoll von einem Notfallmanagement/Business Continuity Management (BCM) ergänzt. Dieser Managementprozess obliegt den Notfallbeauftragten und beinhaltet u. a. die Erstellung folgender Produkte:

- einer Leitlinie zum Notfallmanagement,
- Entwicklung eines Notfallvorsorgekonzeptes sowie
- eines Notfallhandbuches.

Ein vollständiges Notfallmanagement/BCM beschränkt sich nicht nur auf den Ausfall der Ressource Informationstechnik, sondern betrachtet auch den Ausfall der Ressourcen Personal, Infrastruktur (z. B. Gebäude und Anlagen) und Dienstleister. Der Maßnahmenkatalog beschränkt sich auf IT-Notfälle und richtet sich in erster Linie an Geschäftsführer und IT-Verantwortliche in kleinen und mittelständischen Unternehmen, die

- ihren Einstieg in diese Thematik gestalten möchten,
- sich den vielfältigen Bedrohungen aus der voranschreitenden Digitalisierung stellen wollen und
- durch ein IT-Notfallmanagement die Cyber-Resilienz ihres Unternehmens erhöhen wollen.

VORBEREITUNG

- Bestimmen Sie Beauftragte für die Belange der Informationssicherheit und des Notfallmanagements in Ihrem Unternehmen, nach Möglichkeit nicht in Personalunion. Beide arbeiten bei IT-Notfällen eng zusammen.
- Stellen Sie in dem Zusammenhang sicher, dass Ihnen Ihre individuellen und fallbezogenen Erstmaßnahmen im IT-Notfall vorliegen (u. a. Alarmierungs- und Meldewege).
- Identifizieren Sie zeitkritische Geschäftsprozesse und Assets (Kronjuwelen) im Rahmen eines strukturierten Prozesses (Empfehlung: Business Impact Analyse (BIA)) und setzen Sie Schutzmaßnahmen für diese priorisiert um.
- Klären Sie mit Ihren IT-Dienstleistern, für welche IT-Vorfälle Unterstützung gewährt werden kann (Distributed-Denial-of-Service (DDoS), Ransomware, Online-Betrug, Hacking der Webpräsenz, u. a.).
- Identifizieren Sie Dienstleister, die Sie bei IT-Notfällen geeignet unterstützen können und nehmen Sie im Vorfeld Kontakt zu diesen auf.
- Fertigen Sie eine Liste mit allen Ansprechpartnern und treffen Sie Vorabsprachen mit diesen (u. a. Erreichbarkeit, Verfügbarkeit, ggf. Service-Level-Agreement).
- Legen Sie Regeln zur Kommunikation nach innen und außen fest. Eine erfolgreiche Presse- und Öffentlichkeitsarbeit während eines IT-Notfalls kann einen evtl. Imageschaden erheblich begrenzen. Auf diesem Gebiet gibt es Unterstützungsangebote von Dienstleistern. Prüfen Sie vorab, ob Sie solche Angebote in Anspruch nehmen möchten und nehmen Sie frühzeitig Kontakt auf.

Allianz für Cyber-Sicherheit

TOP 12 MASSNAHMEN BEI CYBER-ANGRIFFEN

Diese Fragen sollten Sie sich stellen!

Die Bewältigung eines Cyber-Angriffs ist stets individuell und Maßnahmen müssen auf die Gegebenheiten der IT-Infrastruktur vor Ort, die Art des Angriffs und die Zielsetzungen der Organisation angepasst werden. Die in den 12 als Fragen formulierten Punkten implizierten Maßnahmen dienen als Impuls und Hilfestellung bei der individuellen Bewältigung.

Das Dokument richtet sich an IT-Verantwortliche und Administratoren, in erster Linie in kleinen und mittelständischen Unternehmen.

- Wurden erste Bewertungen des Vorfalls durchgeführt, um festzustellen, ob es sich um einen Cyber-Angriff oder lediglich um einen technischen Defekt handelt?
- Haben Sie kontinuierlich Ihre Maßnahmen abgestimmt, dokumentiert und an alle relevanten Personen und Verantwortlichen kommuniziert?
- Wurden System-Protokolle, Log-Dateien, Notizen, Fotos von Bildschirminhalten, Datenträger und andere digitale Informationen forensisch gesichert?
- Haben Sie stets die besonders zeitkritischen und damit vorrangig zu schützenden Geschäftsprozesse im Fokus gehabt?
- Wurden betroffene Systeme vom Netzwerk getrennt? Wurden Internetverbindungen zu den betroffenen Systemen getrennt? Wurden alle unautorisierten Zugriffe unterbunden?
- Wurden Backups gestoppt und vor möglichen weiteren Einwirkungen geschützt?
- Wurden Maßnahmen unternommen, um das gesamte Maß der Ausbreitung festzustellen? Wurden alle angegriffenen Systeme identifiziert?
- Wurden die beim Cyber-Angriff ausgenutzten Schwachstellen in Systemen oder (Geschäfts-) Prozessen durch relevante Maßnahmen adressiert und behoben?
- Wurden, nach Abstimmung, die Polizei oder relevante Behörden (Datenschutz, Meldepflichten, etc.) benachrichtigt?
- Wurden die Zugangsberechtigungen und Authentisierungsmethoden für betroffene (geschäftliche und ggf. private) Accounts überprüft (z.B. neue Passwörter, 2FA)?
- Wird das Netzwerk nach dem Vorfall weiter überwacht, um mögliche erneute Anomalien festzustellen?
- Wurden die betroffenen Daten und Systeme wiederhergestellt oder neu aufgebaut?

Das Dokument ist ein gemeinsames Produkt nachfolgender Organisationen: Bundeskriminalamt, Charter of Trust, Deutscher Industrie- und Handelskammertag e.V., eco – Verband der Internetwirtschaft e.V., Initiative Wirtschaftsschutz, Nationale Initiative für Informations- und Internet-Sicherheit e.V., VOICE – Bundesverband der IT-Anwender e.V., Allianz für Cyber-Sicherheit des Bundesamtes für Sicherheit in der Informationstechnik

Bundesamt für Sicherheit in der Informationstechnik

Angebote für Unternehmen und Institutionen

NETZWERKE SCHÜTZEN NETZWERKE

www.allianz-fuer-cybersicherheit.de

Informationen erhalten	Erfahrungen austauschen	Kompetenzen erwerben
Online-Informationspool: • BSI-Warnungen • Aktuelle Lagebilder • Lösungshinweise und Anleitungen • Hintergrund-wissen • Veranstaltungs-dokumentation	Cyber-Sicherheits-Tage Cyber-Sicherheits-Web-Talk Podcast Erfahrungsaustausch- und Experten-Kreise	**Angebote der Partner:** • Publikationen • Schulungen, Seminare oder Workshops • Tools • Lizenzen • Dienstleistungen

Bundesamt für Sicherheit in der Informationstechnik

Werden Sie Teil eines starken Netzwerks!

www.allianz-fuer-cybersicherheit.de

Bundesamt
für Sicherheit in der
Informationstechnik

Informationen:

Stefan Becker
Referatsleiter WG22 Cyber-Sicherheit für die Wirtschaft

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