
IMPULSVORTRAG DATENSICHERHEIT UND IT-SECURITY

DATENSICHERHEIT UND IT-SECURITY IM SMART HOME

maixsys[®]

Mediensystemtechnik Aachen

Informationstechnik | Elektrotechnik

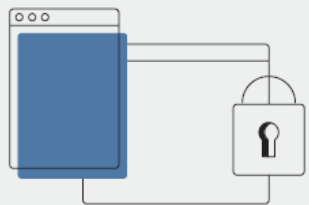
WARUM DATENSICHERHEIT UND IT-SECURITY?

Die Lage der IT-Sicherheit in Deutschland 2023
im Überblick

Ransomware

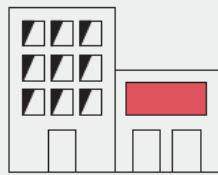
ist weiterhin die größte Bedrohung.

2 Ransomware-Angriffe auf Kommunalverwaltungen oder kommunale Betriebe wurden durchschnittlich pro Monat bekannt.



68 erfolgreiche Ransomware-Angriffe auf Unternehmen wurden bekannt.

15 davon richteten sich gegen IT-Dienstleister.



Mehr als **2.000** Schwachstellen in Softwareprodukten (15 % davon kritisch) wurden im Berichtszeitraum durchschnittlich im Monat bekannt. Das ist ein Zuwachs von 24 %.

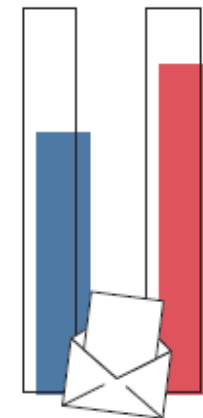


Eine Viertelmillion neue Schadprogramm-Varianten wurden durchschnittlich an jedem Tag im Berichtszeitraum gefunden.



66%

aller Spam-Mails im Berichtszeitraum waren Cyberangriffe:
34 % Erpressungsmails,
32 % Betrugsmails



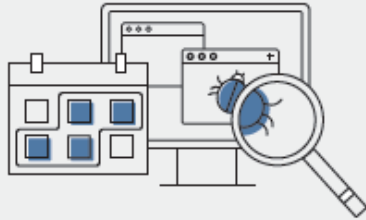
84%

aller betrügerischen E-Mails waren Phishing-E-Mails zur Erbeutung von Authentisierungsdaten, meist bei Banken und Sparkassen.



Quelle: „DIE LAGE DER IT-SICHERHEIT IN DEUTSCHLAND 2023“, BSI

LAGE DER IT-SICHERHEIT IN DEUTSCHLAND 2023

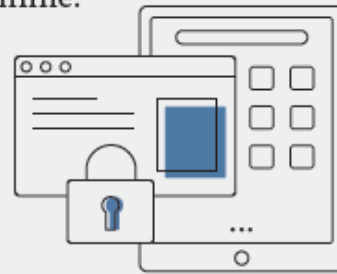


Rund **21.000** infizierte Systeme wurden täglich im Berichtszeitraum erkannt und vom BSI an die deutschen Provider gemeldet.

Durchschnittlich rund **775** E-Mails mit Schadprogrammen wurden an jedem Tag im Berichtszeitraum in deutschen Regierungsnetzen abgefangen.



370 Webseiten wurden im Durchschnitt an jedem Tag des Berichtszeitraums für den Zugriff aus den Regierungsnetzen gesperrt. Der Grund: Die Seiten enthielten Schadprogramme.



Quelle: „DIE LAGE DER IT-SICHERHEIT IN DEUTSCHLAND 2023“, BSI

AUCH DIE HANDWERKKAMMERN SIND BETROFFEN

Industrie- und Handelskammern nach Cyberangriff deutschlandweit offline

Sachverhalt

Der IT-Dienstleister der Industrie- und Handelskammern entdeckte am 3. August 2022 ein auffälliges Verhalten in den bei ihm gehosteten IT-Systemen. Das IHK Cyber Emergency Response Team (IHK-CERT) hat diese Anomalien untersucht. In Zusammenarbeit mit externen IT-Sicherheitsfachleuten wurde entschieden, die Systeme aus Sicherheitsgründen herunterzufahren, um größeren Schaden durch Diebstahl von Daten oder die mögliche Verschlüsselung von Daten zu verhindern.

Dies hatte zur Folge, dass die Verbindung aller 79 Industrie- und Handelskammern in Deutschland zum Internet getrennt wurde und deren Dienste nicht mehr zur Verfügung standen. Dadurch waren Webseiten offline und die Mitarbeitenden weder telefonisch noch per E-Mail erreichbar. Auch interne Anwendungen funktionierten nicht oder nur mit Einschränkungen.

Bewertung

Der Cyberangriff wurde höchstwahrscheinlich von professionellen Angreifern ausgeführt. Deren Vorgehensweise deutet auf Spionage- oder Sabotage-Ziele hin, auch wenn sich eine finanziell ausgerichtete Motivation der Angreifer nicht ausschließen lässt.

Reaktion

Um das Risiko weiterer Angriffe und möglicher Kompromittierungen zu verringern, wurden sämtliche Anwendungen und IT-Systeme erst nach einer intensiven Prüfung schrittweise wieder hochgefahren. Einzelne Kammern und verschiedene Dienstleistungen der Organisation waren auch Monate später noch beeinträchtigt.

Quelle: „DIE LAGE DER IT-SICHERHEIT IN DEUTSCHLAND 2023“, BSI

DATENSICHERHEIT NACH ISO 27001 / BSI GRUNDSCHUTZ

Vertraulichkeit

Verfügbarkeit

Integrität

Standard-
Absicherung

Basis-
Absicherung

Kern-
Absicherung

Kronjuwelen

IT-
Grundschutz-
Bausteine

ISMS

BCMS

Krypto-
konzept

Sicherheits-
organisation

Sicherheits-
konzept

Notfall-
management

DATENSICHERHEIT NACH ISO 27001 / BSI GRUNDSCHUTZ

- Was bedeutet Datensicherheit für mich in der Praxis?

WAS BEDEUTET IT-SICHERHEIT / DATENSICHERHEIT IM UMFELD SMART HOME?

- Wissen Sie, was ein sicheres Passwort ist, und setzen sie dies auch in der Praxis um?
- Welche Geräte werden eingesetzt und wie kommunizieren diese und mit wem?
- Kann ich nachvollziehen, wo welche Daten gespeichert werden?
- Gibt es eine Möglichkeit, dass Unbefugte Zugriff auf das Netzwerk bekommen können?

WAS HEIßT DAS IN DER PRAXIS?

- Datenschutz und IT-Sicherheit ist nicht bequem.
- Awareness schaffen. Aufmerksam sein.
- Den Kunden mitnehmen.
- Geräte aus zweifelhaften Quellen meiden.
- Fit machen bei den grundlegenden IT-Themen, wie WLAN und IP-Netze.
- Klein anfangen und bei Bedarf Experten dazuholen.
- Datensicherheit und IT-Sicherheit sind aus der Praxis nicht mehr wegzudenken und werden in Zukunft immer mehr an Bedeutung gewinnen.

FRAGEN UND ANTWORTEN
VIELEN DANK FÜR IHRE AUFMERKSAMKEIT

Sebastian Biermann

Diplom-Informatiker

geschäftsführender Gesellschafter

maixsys GmbH

biermann@maixsys.de

www.maixsys.de