Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital•Sicher•BSI•

Why SMEs Can Pose a Major Threat to the German Economy…

Manuel Bach, Head of Cybersecurity for SMEs
Federal Office for Information Security / Bundesamt für Sicherheit in der Informationstechnik

Deutsch-Finnisches Business Forum, Rostock, 28. September 2023

Mission Statement

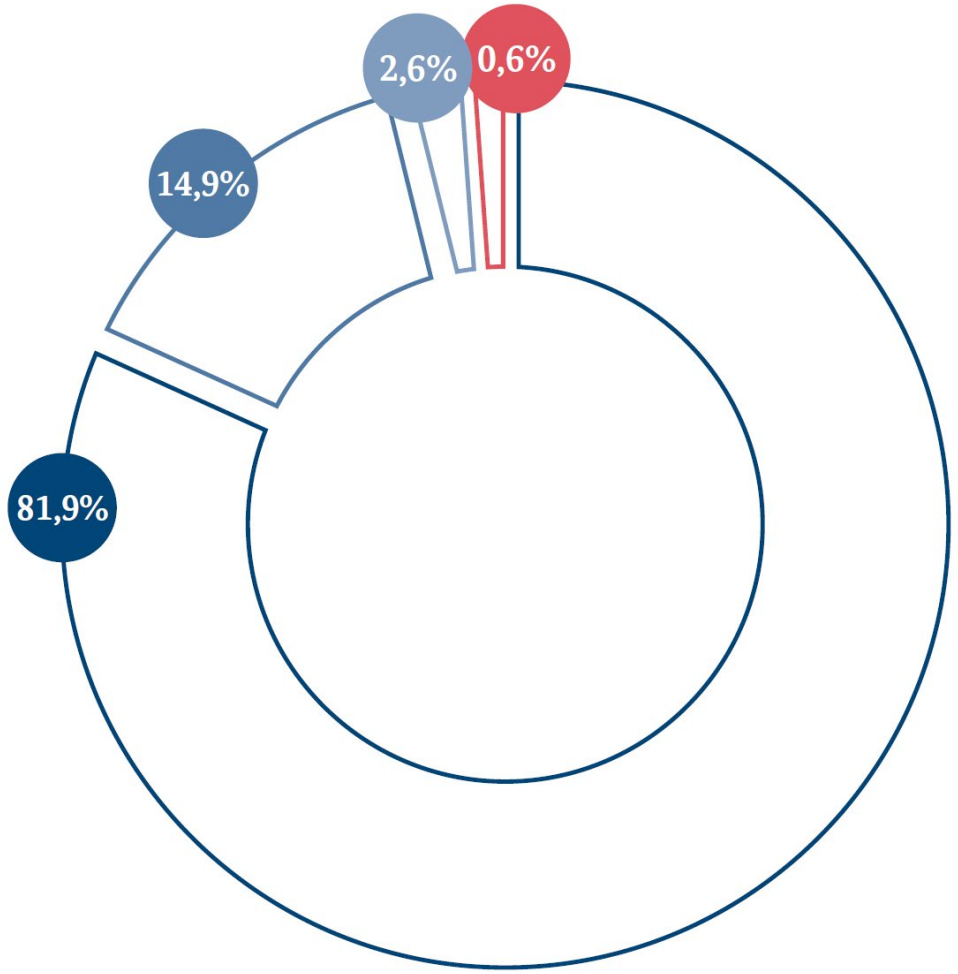
As the federal Germany cyber security authority, the BSI shapes information security in digitalization through prevention, detection and response for the public sector, national industry and society.

Mission Statement

As the federal Germany cyber security authority, the BSI shapes information security in digitalization through **prevention**, detection and response for the public sector, **national industry** and society.

Companies in Germany by Size

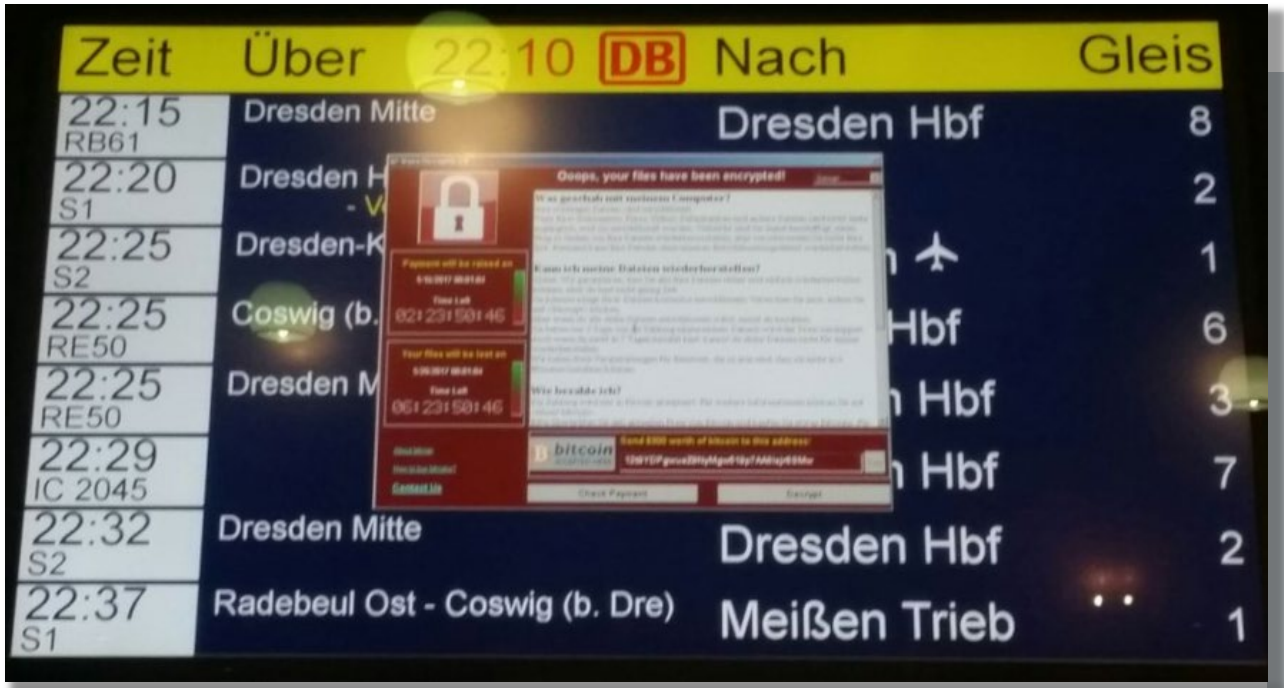
Figures in Percent



- Microenterprises
- Small Enterprises
- Medium Enterprises
- Major Enterprises

- 55% of the 29.4 million employees worked in small and medium-sized enterprises
- SMEs account for 42 % of gross value added


Wana Decrypt0r 2.0
Ooops, your files have been encrypted!
English
What Happened to My Computer?
Your important files are encrypted.
Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.
Can I Recover My Files?
Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.
You can decrypt some of your files for free. Try now by clicking <Decrypt>.
But if you want to decrypt all your files, you need to pay.
You only have 3 days to submit the payment. After that the price will be doubled.
Also, if you don't pay in 7 days, you won't be able to recover your files forever.
We will have free events for users who are so poor that they couldn't pay in 6 months.
How Do I Pay?
Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.
Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.
And send the correct amount to the address specified in this window.
After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am
Payment will be raised on
5/16/2017 00:47:55
Time Left
02:23:57:37
Your files will be lost on
5/20/2017 00:47:55
Time Left
06:23:57:37
About bitcoin
How to buy bitcoins?
Contact Us
bitcoin ACCEPTED HERE
Send $300 worth of bitcoin to this address:
12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw
Copy
Check Payment
Decrypt


Zeit
Über
22:10
DB
Nach
Gleis
22:15 RB61 Dresden Mitte Dresden Hbf 8
22:20 S1 Dresden H 2
22:25 S2 Dresden-K 1
22:25 RE50 Coswig (b. Hbf 6
22:25 RE50 Dresden M Hbf 3
22:29 IC 2045 Hbf 7
22:32 S2 Dresden Mitte Dresden Hbf 2
22:37 S1 Radebeul Ost - Coswig (b. Dre) Meißen Trieb 1

The State of IT Security in Germany in 2021: Overview

RANSOMWARE/DDOS

Significant expansion of cyber-criminal extortion methods

New trend

+ 360% Data leak pages

Hush money blackmail

Ransom blackmail

Protection money blackmail

13 days was the amount of time for which a university hospital was unable to admit emergency patients after a *ransomware* attack

144 million new malware variants

+22% compared to 2020: **117.4 MILLION**

AN AVERAGE OF **394,000** new malware variants every day

2020: 322,000

WITH A PEAK OF **553,000**

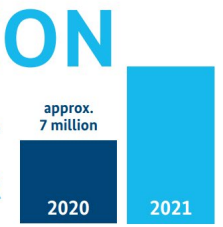
2020: 470,000

TWICE AS MANY *BOT*INFECTIONS ON GERMAN SYSTEMS per day at the daily peak

20,000 > 40,000

98% of all tested systems were susceptible to vulnerabilities in **MS Exchange**

14.8 MILLION reports of malware infections forwarded by the BSI to German network operators, more than **DOUBLE THE NUMBER** of the previous year



44,000 emails containing malware were intercepted per month on average in German government networks

2020 35,000

74,000 websites containing malware programs were blocked by web filters protecting government networks

2020 52,000

Germany among the **TOP THREE NATIONS** in Common Criteria certificates

5,100 MEMBERS OF THE ALLIANCE FOR CYBER SECURITY

- 2020: 4,400
- 2019: 3,700
- 2018: 2,700

< 10% still contained vulnerabilities in **MS Exchange** after warnings from the BSI and Microsoft

Bundesamt
für Sicherheit in der
Informationstechnik

Nationales
IT-Lagezentrum
BSI

SCHWACHSTELLE | GEFÄHRDUNG | VORFALL | IT-ASSETS

Zehntausende deutscher Microsoft Exchange Server haben kritische Sicherheitslücken

CSW-Nr. 2020-252437-1131, Version 1.1, 13.10.2020

IT-Bedrohungslage*: 3 / Orange

Sachverhalt

Seit mehreren Monaten stehen von Microsoft für die unter CVE-2020-0688, CVE-2020-0692 und CVE-2020-16875 geführten Sicherheitslücken des Groupware- und E-Mail-Servers Exchange Sicherheitsupdates bereit [MS2020a, MS2020b, MS2020c].

Bei CVE-2020-0688 handelt es sich um eine Static Key Schwachstelle im Microsoft Exchange Control Panel (ECP) die unter Verwendung eines gestohlenen E-Mail-Kontos die volle Systemkompromittierung ermöglicht. CVE-2020-0692 erlaubt die Eskalation von Privilegien.

Update 1:
Betroffen sind die folgenden Produktversionen, sofern der Einzelpatch zur Behebung der Schwachstelle nicht installiert wurde:

- Microsoft Exchange Server 2010 SP 3 Update RU30 (CVE-2020-0688)
- Microsoft Exchange Server 2013 Cummulative Update 23
- Microsoft Exchange Server 2016 Cummulative Update 14 und 15
- Microsoft Exchange Server 2019 Cummulative Update 3 und 4

Ebenso betroffen sind ältere Produktversionen.

Bei CVE-2020-16875 handelt es sich um eine durch die fehlerhafte Argument-Validierung des New-DlpPolicy cmdlet bedingte Sicherheitslücke, die nach vorheriger Authentisierung ebenfalls Remote Code Execution erlaubt.

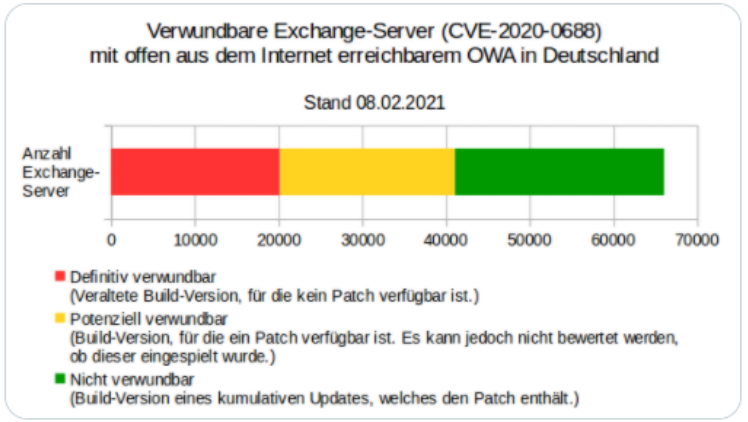
Update 1:
Betroffen sind die folgenden Produktversionen, sofern der Einzelpatch zur Behebung der Schwachstelle nicht installiert wurde:

* 1 / Grau: Die IT-Bedrohungslage ist ohne wesentliche Auffälligkeiten auf anhaltend hohem Niveau.
2 / Gelb: IT-Bedrohungslage mit verstärkter Beobachtung von Auffälligkeiten unter temporärer Beeinträchtigung des Regelbetriebs.
3 / Orange: Die IT-Bedrohungslage ist geschäftskritisch. Massive Beeinträchtigung des Regelbetriebs.
4 / Rot: Die IT-Bedrohungslage ist extrem kritisch. Ausfall vieler Dienste, der Regelbetrieb kann nicht aufrecht erhalten werden.

BSI-Cyber-Sicherheitswarnung

CERT-Bund @certbund · 9. Feb.

Ein Jahr nach Veröffentlichung des #Sicherheitsupdates sind noch immer mindestens 31% (potenziell bis zu 63%) der #Exchange-Server in Deutschland mit offen aus dem Internet erreichbarem #OWA für die kritische #Schwachstelle CVE-2020-0688 verwundbar.



6 47 42

Bundesamt
für Sicherheit in der
Informationstechnik

Nationales
IT-Lagezentrum
BSI

SCHWACHSTELLE | GEFÄHRDUNG | VORFALL | IT-ASSETS

Mehrere Schwachstellen in MS Exchange

Nr. 2021-197772-1500, Version 1.5, 08.03.2021

IT-Bedrohungslage*: 4 / Rot

Sachverhalt

In der Nacht zum Mittwoch, den 3. März 2021, hat Microsoft Out-of-Band Updates für Exchange Server veröffentlicht. Hiermit werden vier Schwachstellen geschlossen, die in Kombination bereits für zielgerichtete Angriffe verwendet werden und Tätern die Möglichkeit bieten, Daten abzugreifen oder weitere Schadsoftware zu installieren.

Bei den Schwachstellen handelt es sich um:

- CVE-2021-26855 ist eine server-side request forgery (SSRF) Schwachstelle in Exchange, welche es einem Angreifer erlaubt, HTTP-Requests zu senden und sich am Exchange-Server zu authentisieren.
- CVE-2021-26857 ist eine insecure deserialization Schwachstelle im Unified Messaging Service. Bei insecure deserialization werden Nutzer-bestimmte Daten von einem Programm deserialisiert. Hierüber ist es möglich, beliebigen Programmcode als SYSTEM auf dem Exchange-Server auszuführen. Dies erfordert Administrator-Rechte oder die Ausnutzung einer entsprechenden weiteren Schwachstelle.
- CVE-2021-26858 und CVE-2021-27065 sind Schwachstellen, mit denen – nach Authentisierung – beliebige Dateien auf dem Exchange-Server geschrieben werden können. Die Authentisierung kann z. B. über CVE-2021-26855 oder abgeflossene Administrator-Zugangsdaten erfolgen.

Nach Angaben des Herstellers richteten sich die Angriffe gegen amerikanische Forschungseinrichtungen mit Pandemie-Fokus, Hochschulen, Anwaltsfirmen, Organisationen aus dem Rüstungssektor, Think Tanks und NGOs. Microsoft vermutet hinter den Vorfällen eine staatliche Hackergruppe aus China, die HAFNIUM genannt wird.

Namen der ursprünglichen Opfer sind im BSI nicht bekannt. Bei den beobachteten Angriffen wurde hierüber Zugang zu den E-Mail-Accounts erlangt, sowie weitere Malware zur Langzeit-Persistenz installiert [MIC2021a].

Die Attacken erfordern die Möglichkeit, eine nicht-vertrauenswürdige Verbindung (z.B. aus dem Internet) auf Port 443 zu dem Exchange-Server zu etablieren. Daher sind Server geschützt, welche nicht-vertrauenswürdige Verbindungen beschränken oder nur per VPN erreichbar sind. Diese Lösung schützt

* 1 / Grau: Die IT-Bedrohungslage ist ohne wesentliche Auffälligkeiten auf anhaltend hohem Niveau.
2 / Gelb: IT-Bedrohungslage mit verstärkter Beobachtung von Auffälligkeiten unter temporärer Beeinträchtigung des Regelbetriebs.
3 / Orange: Die IT-Bedrohungslage ist geschäftskritisch. Massive Beeinträchtigung des Regelbetriebs.
4 / Rot: Die IT-Bedrohungslage ist extrem kritisch. Ausfall vieler Dienste, der Regelbetrieb kann nicht aufrecht erhalten werden.

BSI-IT-Sicherheitswarnung

If the following statement applies to you, please raise your hand!

#1

I have the skills necessary to operate a vacuum cleaner and clean a toilet!

#2

I hired someone to operate our vacuum cleaner and clean our toilet!

#3

I have the skills necessary to create immutable backups, keep all systems up to date with the latest patches, ensure secure configuration of applications, optimize firewall rules, detect network anomalies, identify, isolate and clean malware infested systems, redeploy systems and apply a current backup in a timely manner!

#4

I hired someone who has the skills necessary to create immutable backups, keep all systems up to date with the latest patches, ensure secure configuration of applications, optimize firewall rules, detect network anomalies, identify, isolate and clean malware infested systems, redeploy systems and apply a current backup in a timely manner!

Keep you systems up to date!!!

Create Immutable Backups!!!!

Phishing Attacks

Countermeasures

- Long, complex, new passwords
- A separate password per account
- Password manager
- Two-factor authentication
- Passkeys

The Washington Post
Democracy Dies in Darkness

Man really did hack Trump's Twitter account by guessing password, 'maga2020!,' Dutch prosecutors say

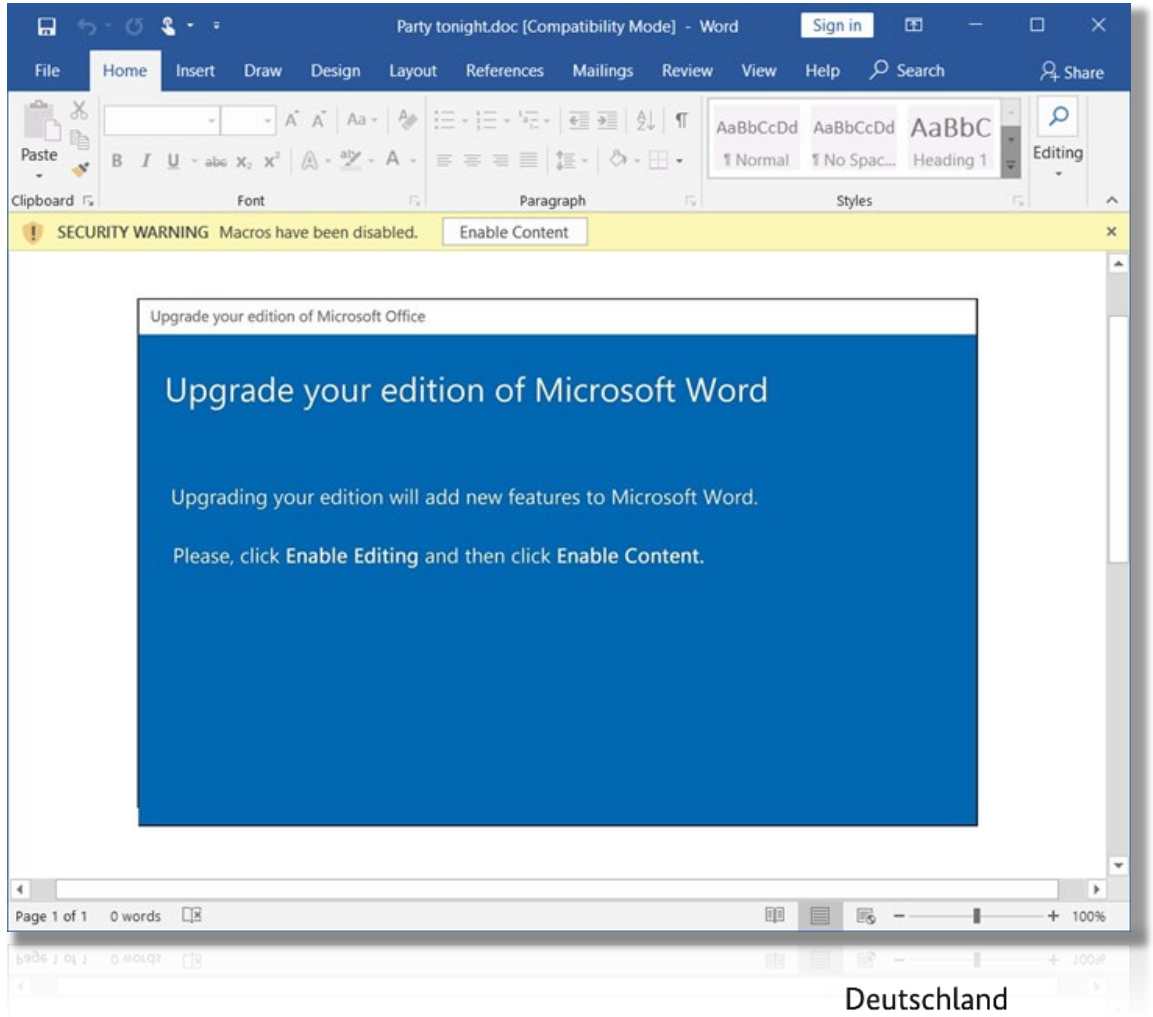
By Miriam Berger
December 17, 2020 at 12:02 p.m. EST

President Trump's Twitter account. (J. David Ake/AP)

Typical Attack via Macros

Countermeasure (free of charge):

- Disable the execution of macros in the Windows group policies.
- If macros are absolutely required, allow only signed macros.



Make use of the BSI !

DIN SPEC 27076:2023-02
„IT Security Consulting for Small and Micro Enterprises “

For SMEs:

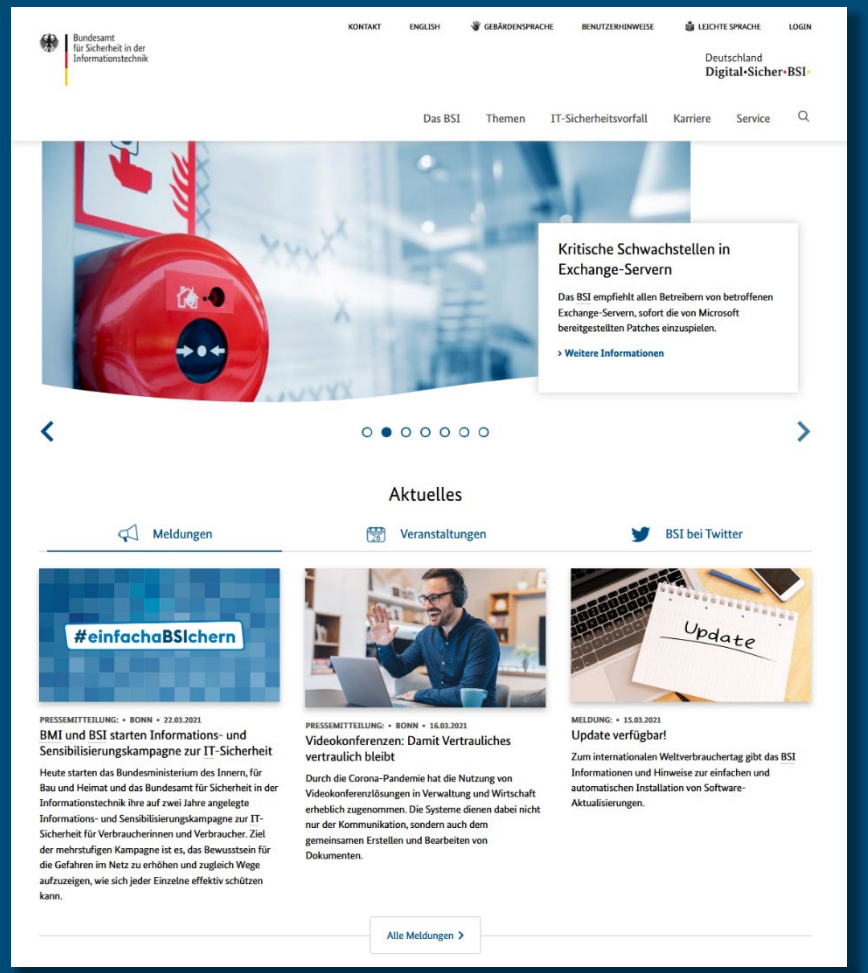
- Ideal, low-threshold entry into corporate IT protection
- Substantial public subsidies (federal/state/local governments)

For IT service providers:

Free use of a web-based software provided by the BSI for conducting the CyberRisikCheck and preparing the advisory reports

For more information, visit:
www.bsi.bund.de/dok/crc

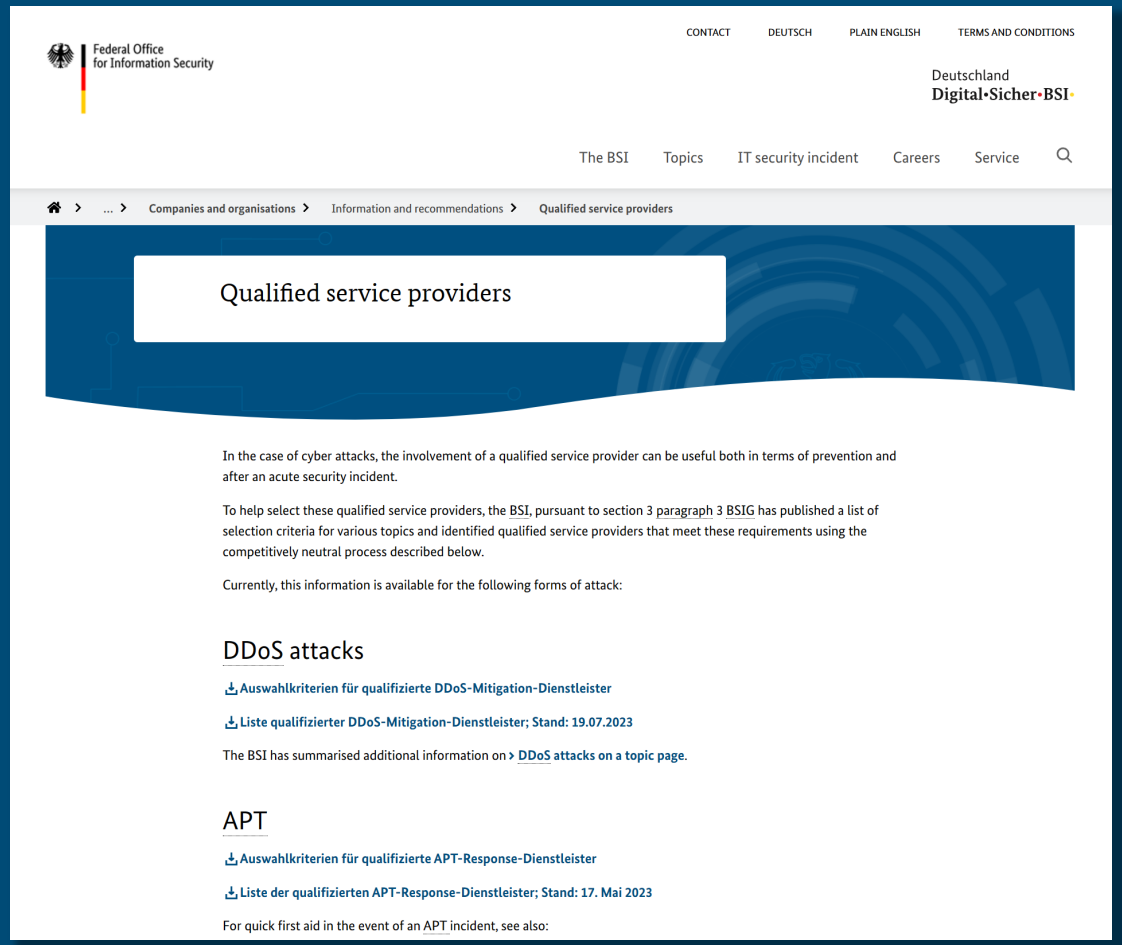
Cyber security colloquially explained at a simple level.



Direct link to offer for SMEs:

www.bsi.bund.de/kmu

- Tips & tricks for SMEs
- Contact option for security incidents
- Subscription option for an SME newsletter



Federal Office for Information Security

CONTACT DEUTSCH PLAIN ENGLISH TERMS AND CONDITIONS

Deutschland Digital•Sicher•BSI•

The BSI Topics IT security incident Careers Service

... > Companies and organisations > Information and recommendations > Qualified service providers

Qualified service providers

In the case of cyber attacks, the involvement of a qualified service provider can be useful both in terms of prevention and after an acute security incident.

To help select these qualified service providers, the BSI, pursuant to section 3 paragraph 3 BSIG has published a list of selection criteria for various topics and identified qualified service providers that meet these requirements using the competitively neutral process described below.

Currently, this information is available for the following forms of attack:

DDoS attacks

Auswahlkriterien für qualifizierte DDoS-Mitigation-Dienstleister

Liste qualifizierter DDoS-Mitigation-Dienstleister; Stand: 19.07.2023

The BSI has summarised additional information on > DDoS attacks on a topic page.

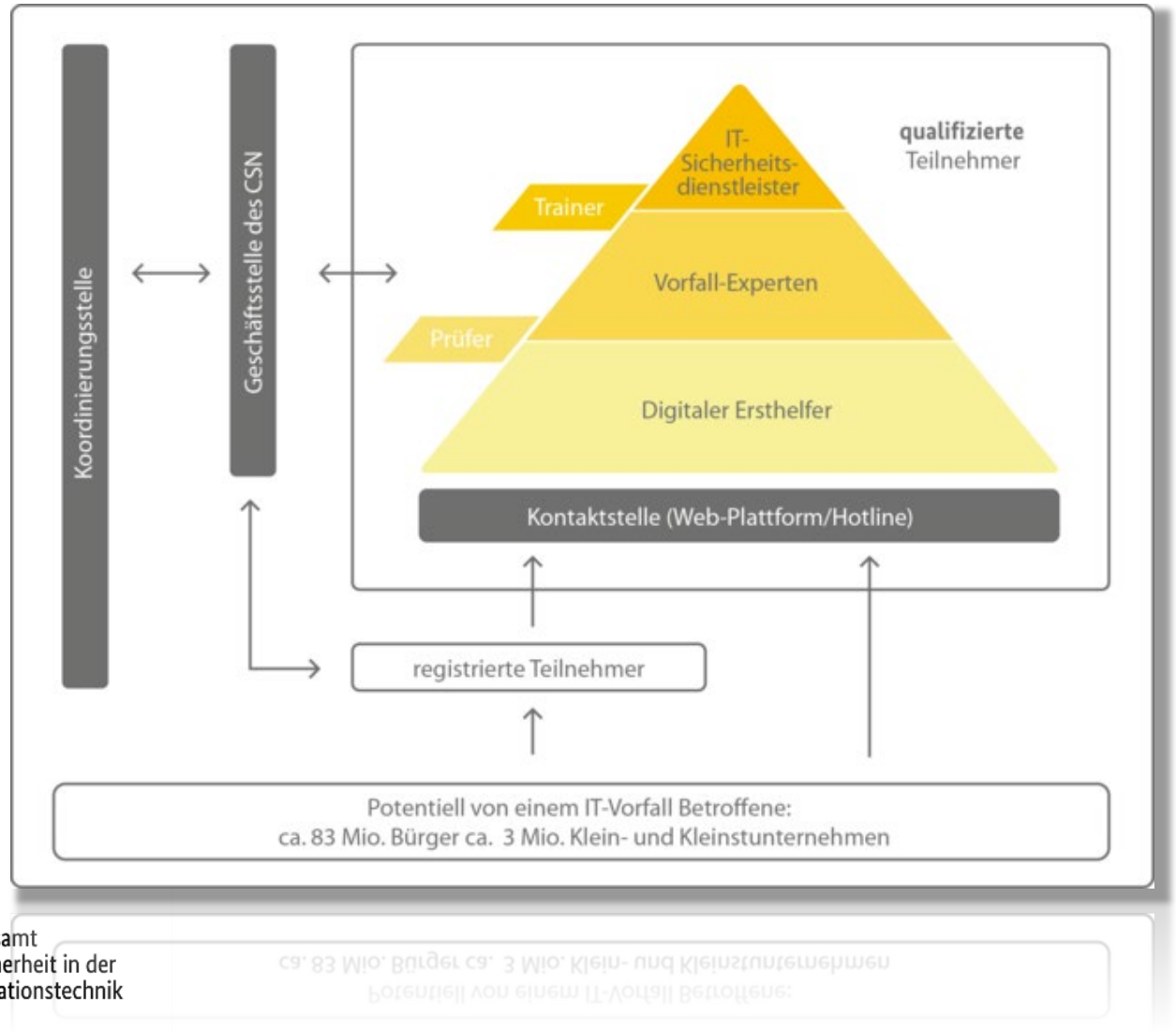
APT

Auswahlkriterien für qualifizierte APT-Response-Dienstleister

Liste der qualifizierten APT-Response-Dienstleister; Stand: 17. Mai 2023

For quick first aid in the event of an APT incident, see also:

Cyber Security Network



- Affected parties receive support from qualified participants of the cyber security network following an IT security incident
- Trainers and examiners support the qualification concept and ensure the quality of the supporting service offering through training and the taking of an examination respectively.
- The cyber security network is closely interlinked with the Alliance for Cyber Security and complements its offering with its reactive service.

https://www.bsi.bund.de/Cyber-Sicherheitsnetzwerk

Create a Network – Alliance for Cyber Security

The Alliance for Cyber Security is an initiative of the German Federal Office for Information Technology (BSI). It provides a basis for cooperation between:

- State,
- industry,
- manufacturers and
- Research

www.allianz-fuer-cybersicherheit.de

Thank you for your attention!

Deutschland
Digital•Sicher•BSI•

Contact Information

Manuel Bach
Head of Cybersecurity for SMEs (Unit WG 23)
manuel.bach@bsi.bund.de
Tel. +49 (0) 228 9582 5941
Fax +49 (0) 228 10 9582 5941

Bundesamt für Sicherheit in der Informationstechnik (BSI)
Godesberger Allee 185-189
53175 Bonn
www.bsi.bund.de

Bundesamt
für Sicherheit in der
Informationstechnik