IT Security in Zahnarztpraxen

Wenn Würmer, Viren und Trojaner die Patientendossiers zerstören!

CDS
BAUSOFTWARE
BAUINGENIEURE
NETCOM

Vorstellung

- Marco Dornig
- Stv. Leiter CDS Netcom
- Beratung von KMU’s

CDS
BAUSOFTWARE
BAUINGENIEURE
NETCOM

Agenda

- Einstieg
- Bedrohungen
- Wie können wir uns schützen?
- Exkursion ins «dunkle» Internet
- Fragen?

CDS
BAUSOFTWARE
BAUINGENIEURE
NETCOM

Home › Security › Alle Themen › Hacking › 65 Prozent mehr Cyberattacken in der Sch...

Jahresvergleich von Check Point 11.01.2022, 08:04 Uhr

65 Prozent mehr Cyberattacken in der Schweiz

Trauriger Rekord: Die Zahl der Cyberangriffe ist 2021 in der Schweiz dramatisch gestiegen. Die Sicherheitsforscher von Check Point haben hierzulande im Vergleich zum Vorjahr 65 Prozent mehr Attacken registriert.

Wind turbine firm Nordex hit by Conti ransomware attack

By Lawrence Abrams

April 14, 2022 09:54 PM 0

Image: Nordex

The Conti ransomware operation has claimed responsibility for a cyberattack on wind turbine giant Nordex, which was forced to shut down IT systems and remote access to the managed turbines earlier this month.

Studie: Über 3000 Schweizer Unternehmen haben bereits Kundendaten verloren

Von Thomas Schwendener mit Material von Keystone-sda, 8. Dezember 2020, 15:36

SECURITY KMU STUDIE CORONAVIRUS DATENSCHUTZ DIGITALSWITZERLAND VERBAND NCSC SATW MOBILIAR SCHWEIZ

Foto: Ekaterina Tyapkina / Unsplash

Die KMU der Schweiz glauben sich gerüstet gegen Cyberangriffe. Ihre grosse Schwäche ist aber die mangelnde Schulung der Mitarbeitenden.

Startseite › Wirtschaft › Lösegeld - Nach Cyber-Angriff: Erpresser erhöhen Druck auf Peter Spuhlers Stadler Rail

LÖSEGELD

Nach Cyber-Angriff: Erpresser erhöhen Druck auf Peter Spuhlers Stadler Rail

Die Cyberkriminellen, die Anfang Mai ins IT-Netzwerk des Schienenfahrzeugbauers Stadler eingedrungen sind, haben mutmasslich einen zweiten Teil der gestohlenen Daten im Darknet veröffentlicht. Sie wollen ein Lösegeld erpressen, beissen aber auf Granit.

Thomas Griesser Kym
06.07.2020, 14.35 Uhr

Merken Drucken Teilen

Home › Security › Alle Themen › Hacking › 65 Prozent mehr Cyberattacken in der Sch...

Jahresvergleich von Check Point 11.01.2022, 08:04 Uhr

65 Prozent mehr Cyber... Schweiz

Trauriger Rek...

Hafnium-Angri... Server betriff...

Wohl seit Wochen greift die chinesi... über eine Schwachstelle an. Nun gi...

Es werden Hackerangriffe au...

CVE-2022-30190 (Follina) vulnerability in MSDT: description and counteraction

INCIDENTS 06 JUN 2022 2 minute read

// AUTHORS

AMR

At the end of May, researchers from the nao_sec team reported a new zero-day vulnerability in Microsoft Support Diagnostic Tool (MSDT) that can be exploited using Microsoft Office documents. It allowed attackers to remotely execute code on Windows systems, while the victim could not even open the document containing the exploit, or open it in Protected Mode. The vulnerability, which the researchers dubbed Follina, later received the identifier CVE-2022-30190.

Table of Contents

CVE-2022-30190 technical details

Protecting against Follina

GREAT WEBINARS

13 MAY 2021, 1:00PM
GReAT Ideas. Balalaika Edition
BORIS LARIN, DENIS LEGEZO

26 FEB 2021, 12:00PM
GReAT Ideas. Green Tea Edition
JOHN HULTQUIST, BRIAN BARTHOLOMEW, SUGURU ISHIMARU, VITALY KAMLUK, SEONGSU PARK, YUSUKE NIWA, MOTOHIKO SATO

17 JUN 2020, 1:00PM
GReAT Ideas. Powered by SAS: malware attribution and next-gen IoT honeypots

Image: Nordex

The Conti ransomware operation has claimed responsibility for a cyberattack on wind turbine giant Nordex, which was forced to shut down IT systems and remote access to the managed turbines earlier this month.

Studie: Über 3000 Schweizer Unternehmen haben bereits Kundendaten verloren

Von Thomas Sc... ...dener mit Material von Keystone-sda, 8. Dezember 2020, 15:36

SECURITY ...NAVIRUS DATENSCHUTZ DIGITALSWITZERLAND VERBAN...

Von Philipp...

Log4Shell-Lücke: Das sagen die Entwickler von Log4j

...er 2021, 17:39

...ERNATIONAL DEVELOPER OPEN SOURCE APACHE

...veizer Erfinder der Java-...otfallstunden berichten aktuelle

mutmasslich einen zweiten Teil... veröffentlicht. Sie wollen ein Lösegeld erpr... Granit.

Thomas Griesser Kym
06.07.2020, 14.35 Uhr

Merken Drucken Teilen

- Übersichtlichkeit der Infrastrukturen durch Wachstum sinkt
- Komplexität durch zunehmende App-Vielfalt
- Zunehmende Flexibilität (Hybrid Workplace)
- Wald aus verschiedensten Lösungen
- Ständige Anpassungen des Datenschutzgesetzes
- Bedrohungen verändern sich

Wie schützen Sie sich vor Cyberkriminalität?

CDS
BAUSOFTWARE
BAUINGENIEURE
NETCOM

CDS
BAUSOFTWARE
BAUINGENIEURE
NETCOM

Viel zu teuer!

Ich bin dagegen versichert!

Viel zu komplex!

Unsere Daten interessieren niemanden!

Tatsächliche Aussagen der Schweizer KMU's

Wir sind dafür nicht aufgestellt!

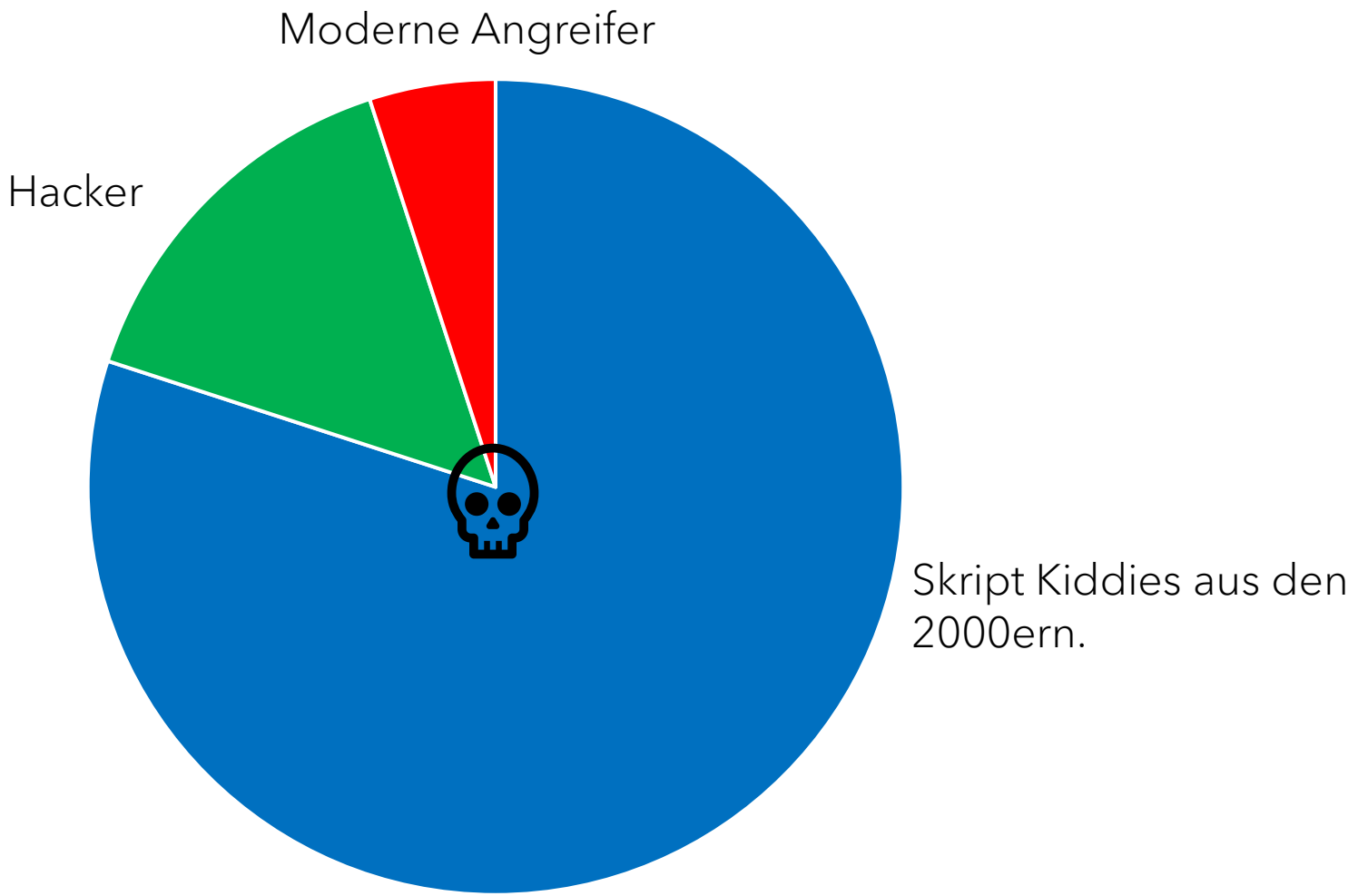
Firewall und AntiVirus reichten schon immer!

CDS
BAUSOFTWARE
BAUINGENIEURE
NETCOM

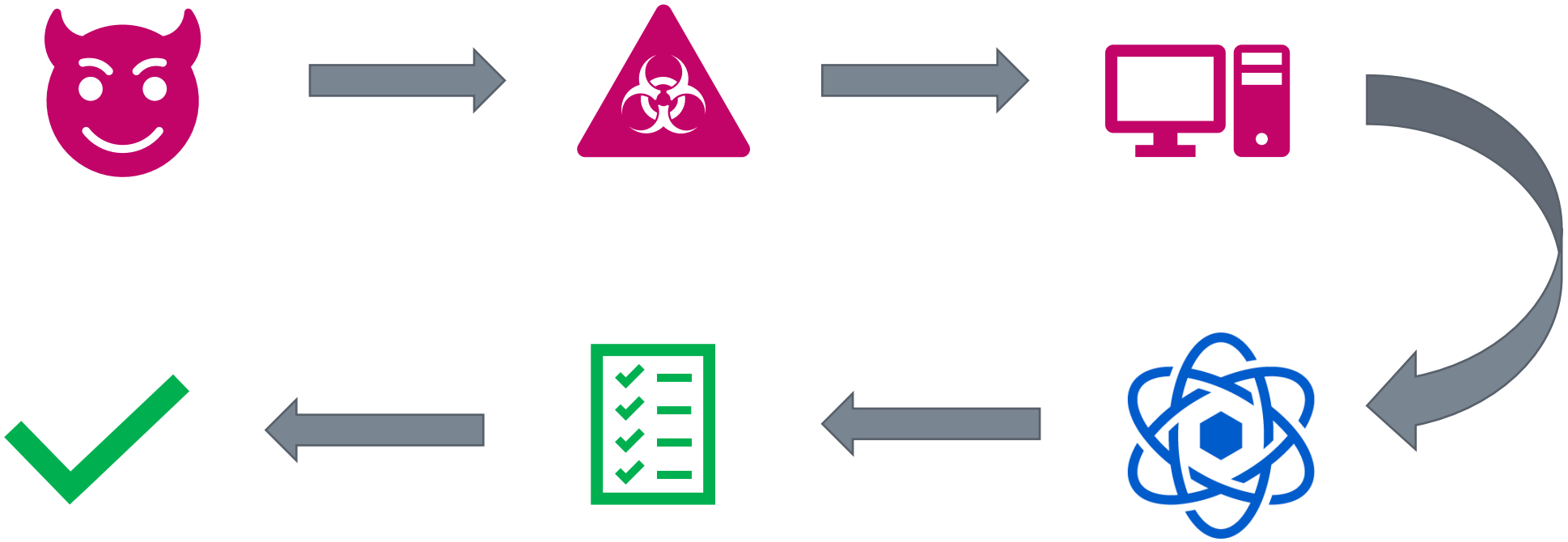
Bedrohungen verändern sich!

CDS
BAUSOFTWARE
BAUINGENIEURE
NETCOM

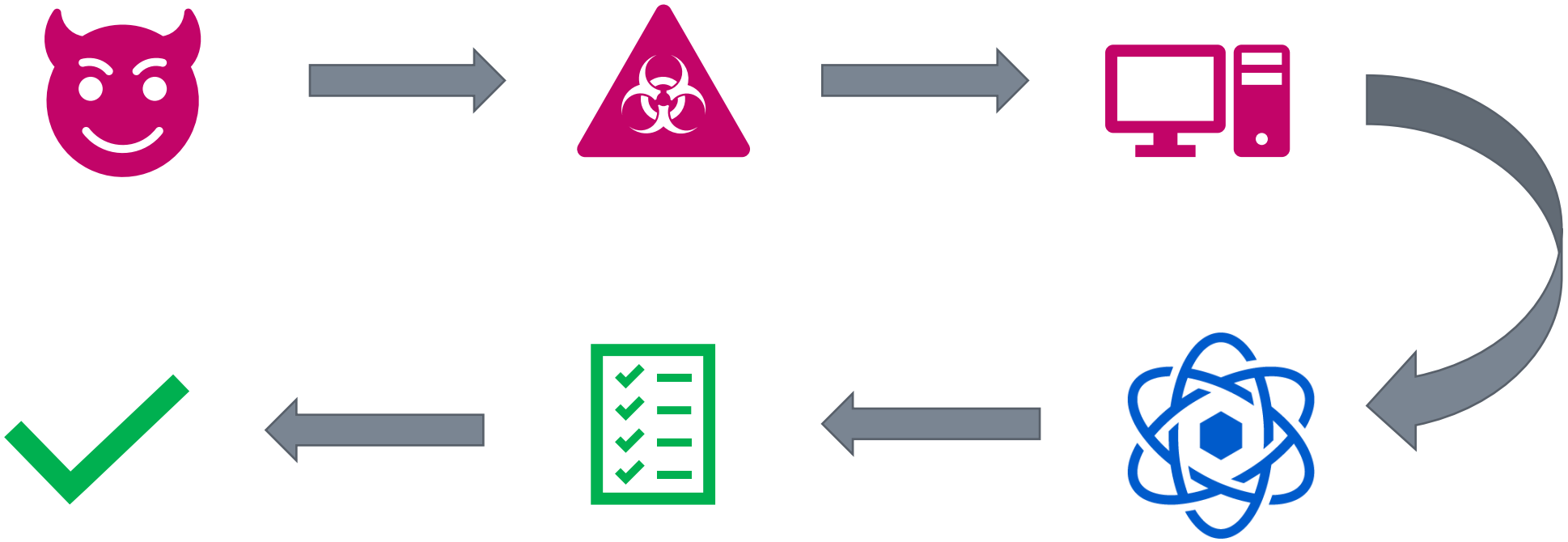
Bedroher von vor 20 Jahren



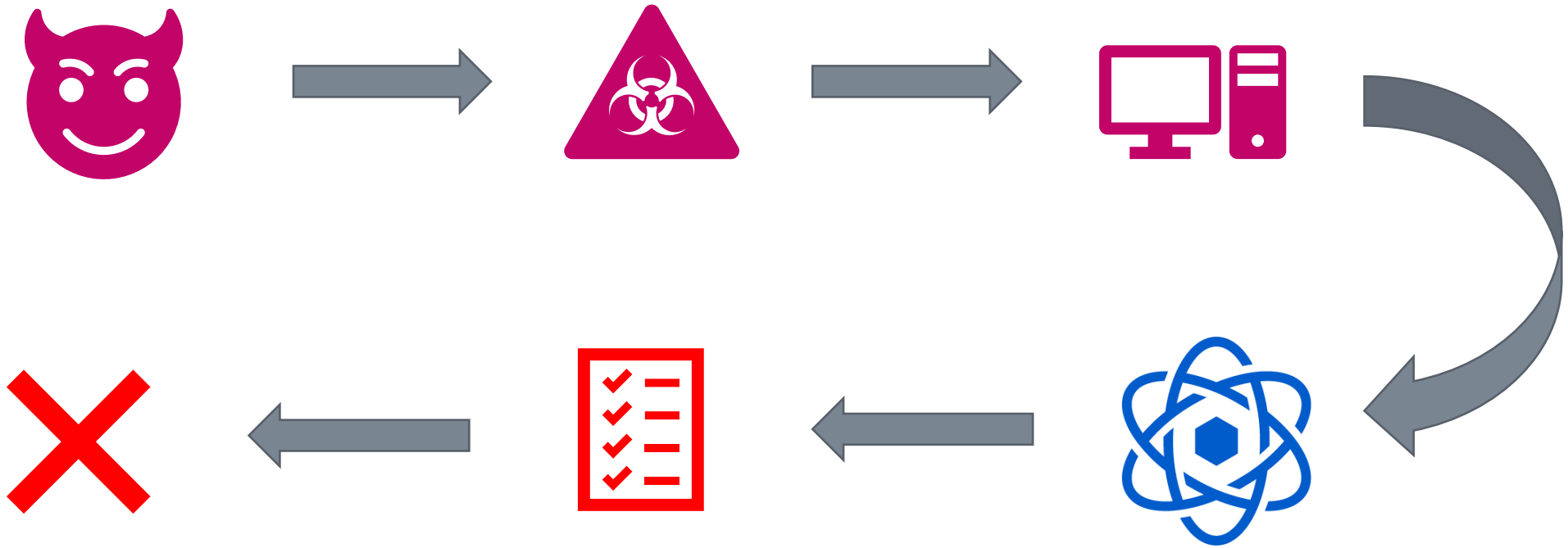
CDS
BAUSOFTWARE
BAUINGENIEURE
NETCOM



CDS
BAUSOFTWARE
BAUINGENIEURE
NETCOM



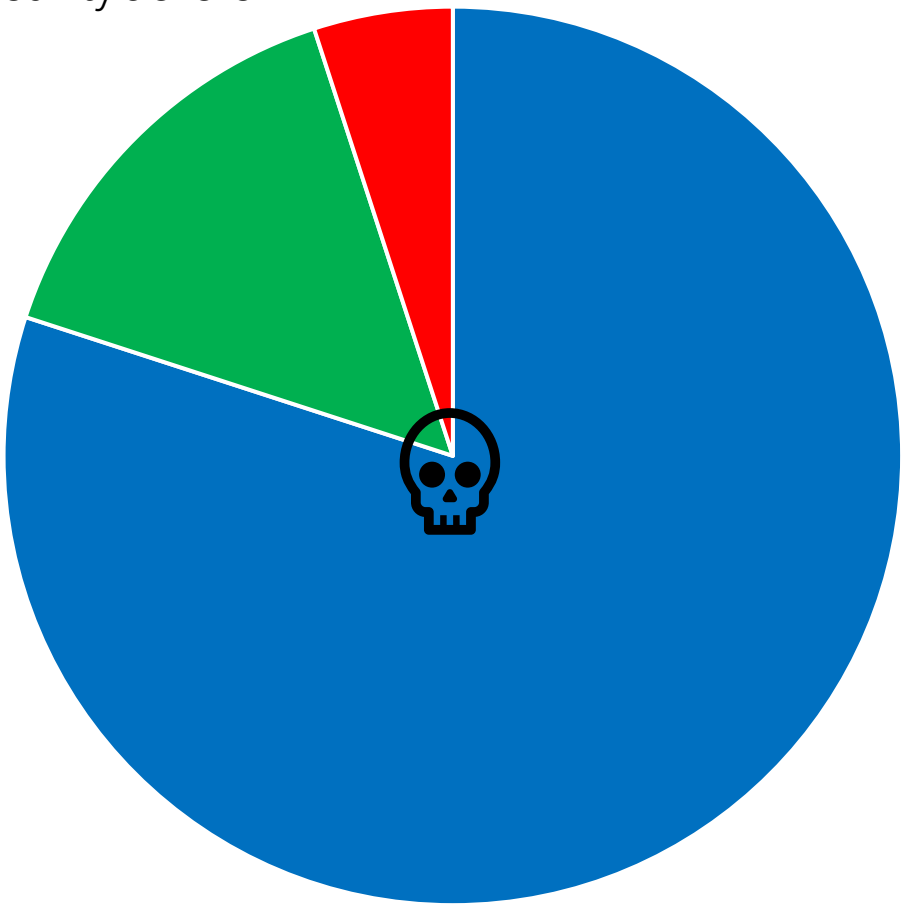
CDS
BAUSOFTWARE
BAUINGENIEURE
NETCOM



CDS
BAUSOFTWARE
BAUINGENIEURE
NETCOM

Was nützte gegen diese Bedrohungen

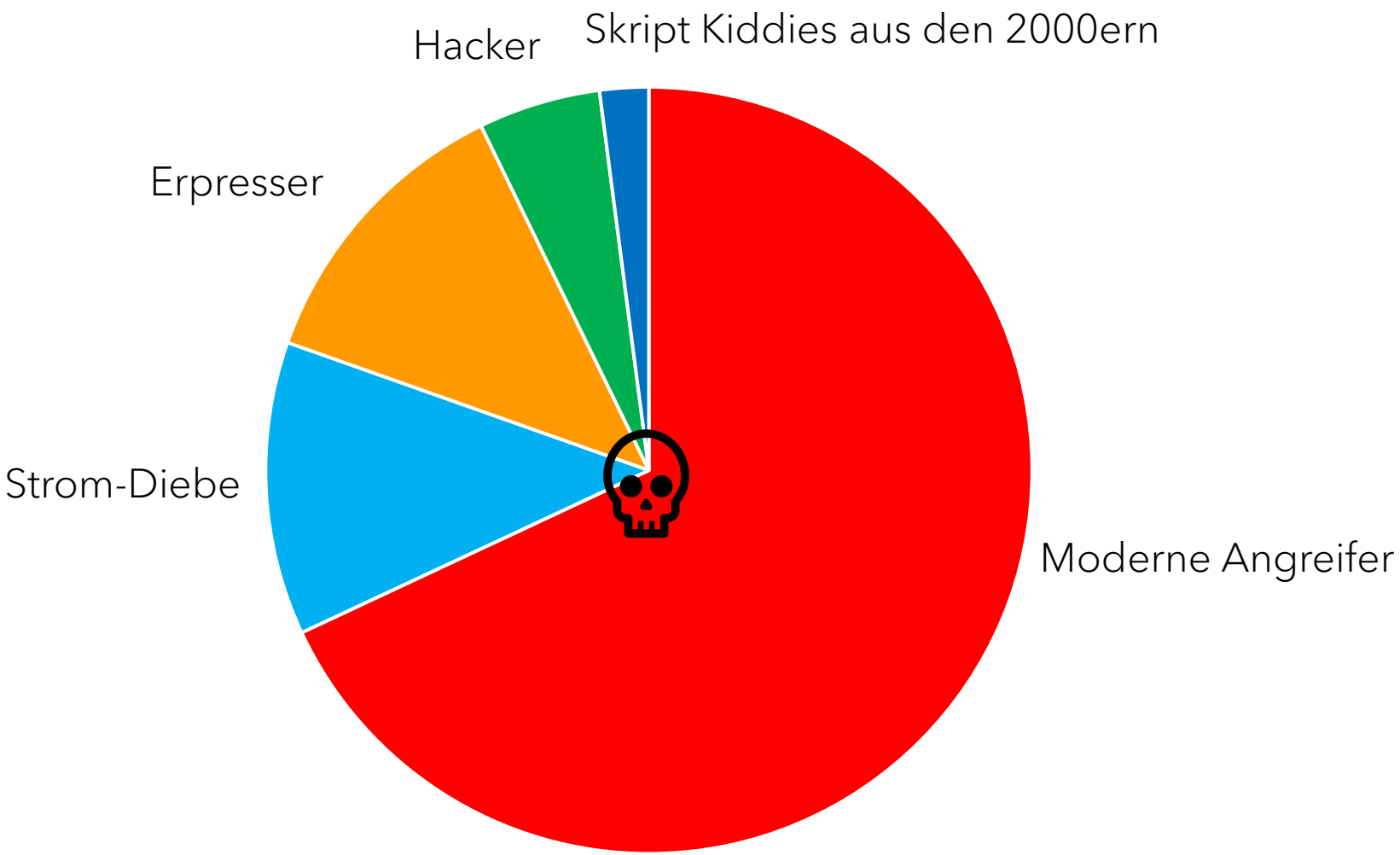
KnowHow im Securitybereich



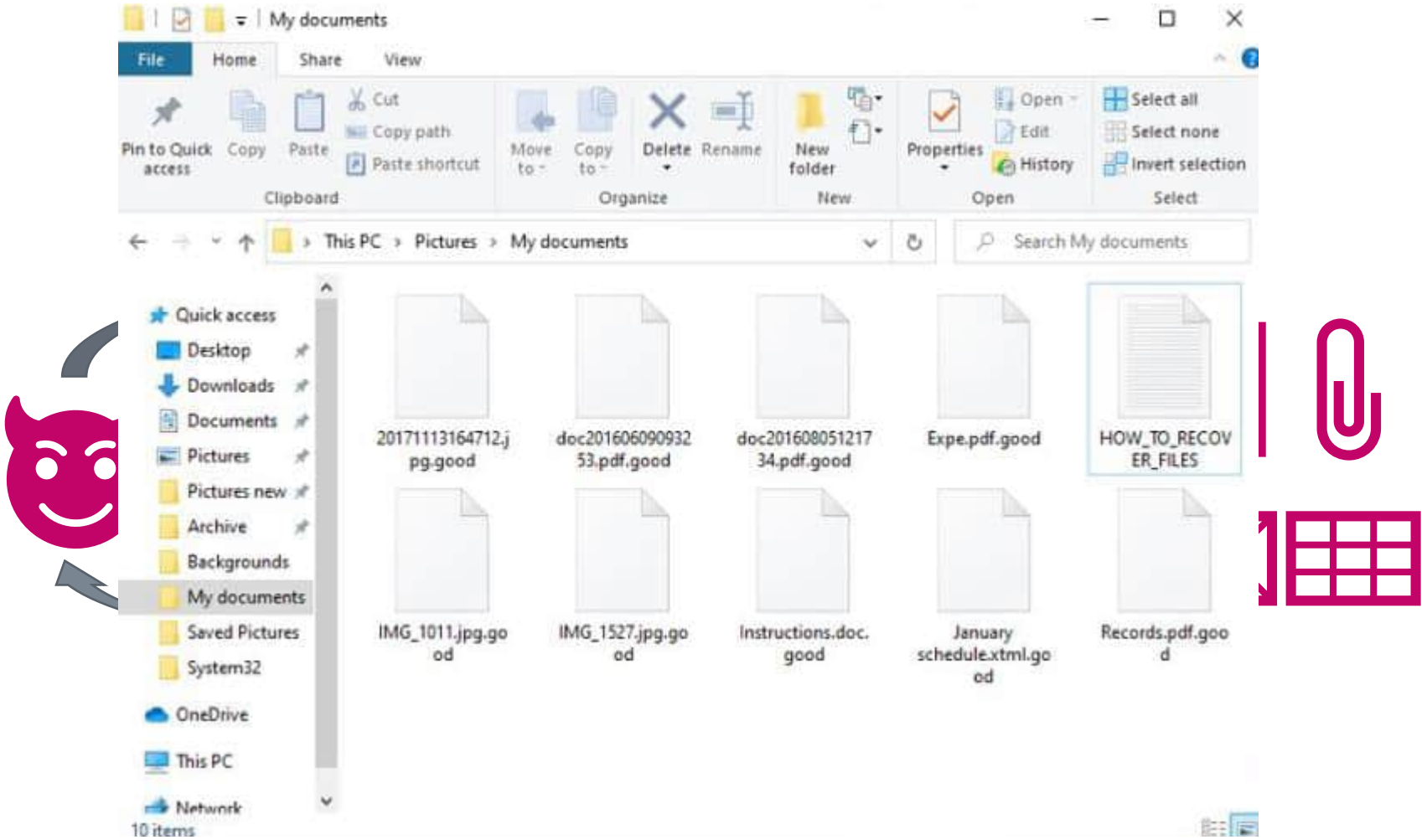
AntiVirus

CDS
BAUSOFTWARE
BAUINGENIEURE
NETCOM

Bedroher von Heute

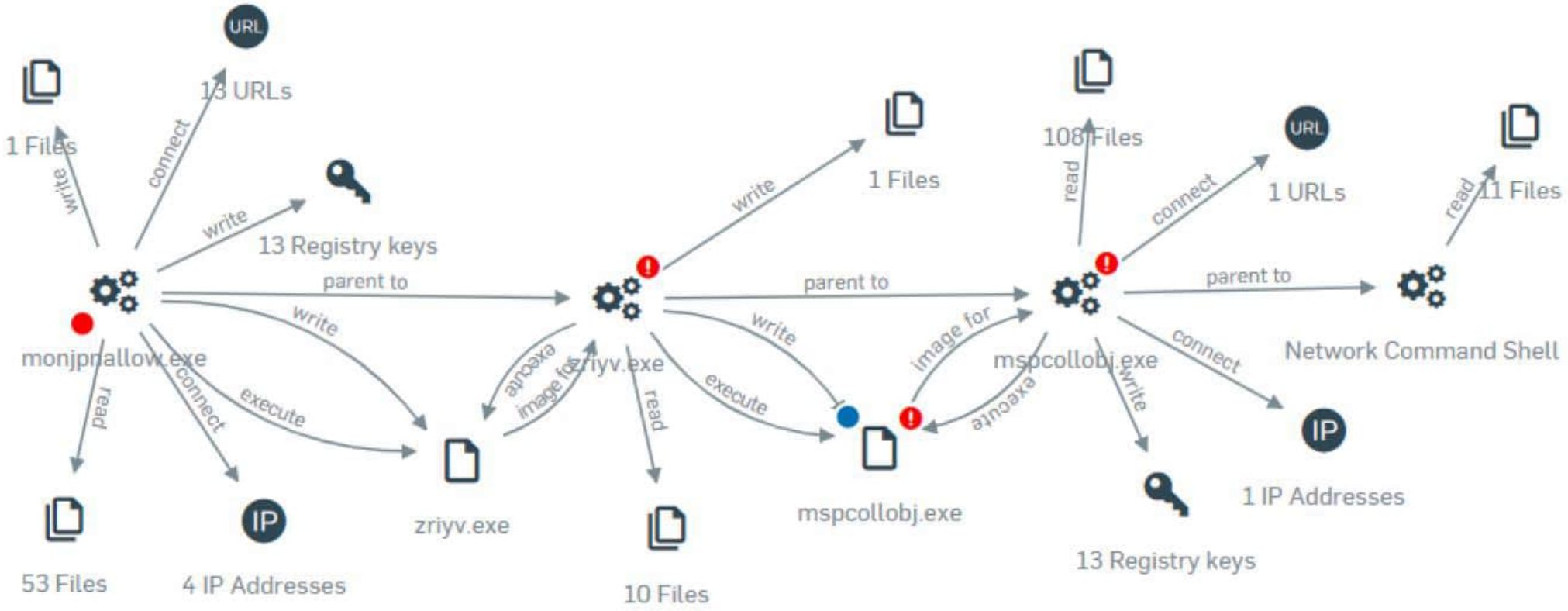


CDS
BAUSOFTWARE
BAUINGENIEURE
NETCOM



CDS
BAUSOFTWARE
BAUINGENIEURE
NETCOM

CDS
BAUSOFTWARE
BAUINGENIEURE
NETCOM

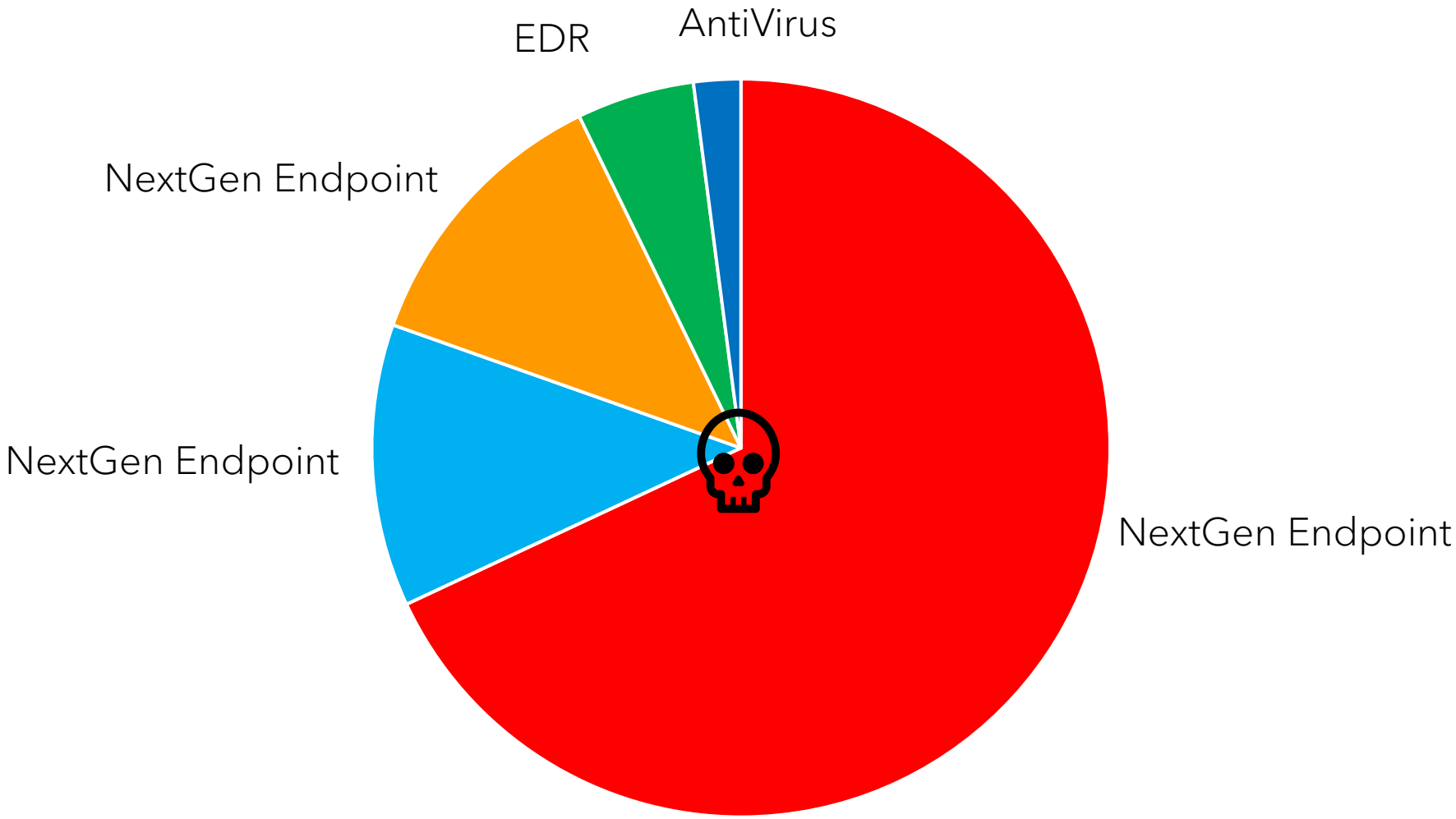


CDS
BAUSOFTWARE
BAUINGENIEURE
NETCOM

- Antivirus als solches genügt nicht mehr
- Benötigt Next-Gen Engine
- Deep Learning / Verhaltensanalyse
- Cloud und Big Data

= Zero Day Erkennung / Erkennung einer Bedrohung vom ersten Tag an.

Was nützt heute?



CDS
BAUSOFTWARE
BAUINGENIEURE
NETCOM

Wie können Sie sich einfach schützen?

CDS
BAUSOFTWARE
BAUINGENIEURE
NETCOM

123456
password
12345678
12341234
1asdasdasdasd
Qwertz123
Password1
123456789
Qwertz1
12345678secret
Abc123
111111
stratfor
lemonfish
sunshine
123123123
1234567890
Password123
123123
1234567

https://haveibeenpwned.com/

gehacktemail@gmail.com pwned?

Oh no — pwned!

Pwned in 6 data breaches and found 1 paste (subscribe to search sensitive breaches)

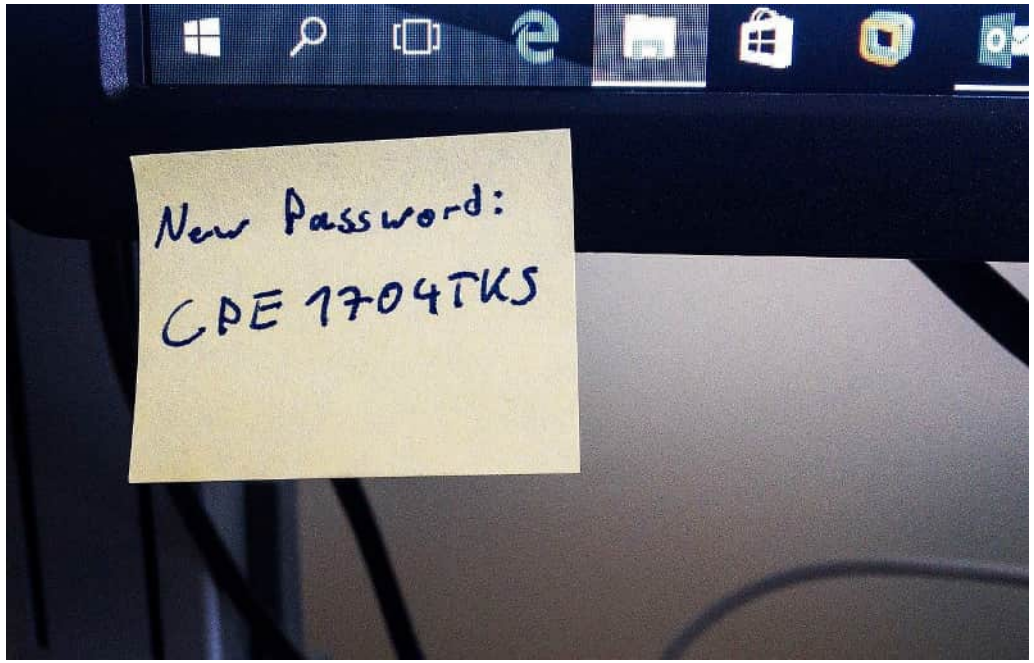
3 Steps to better security

Start using 1Password.com

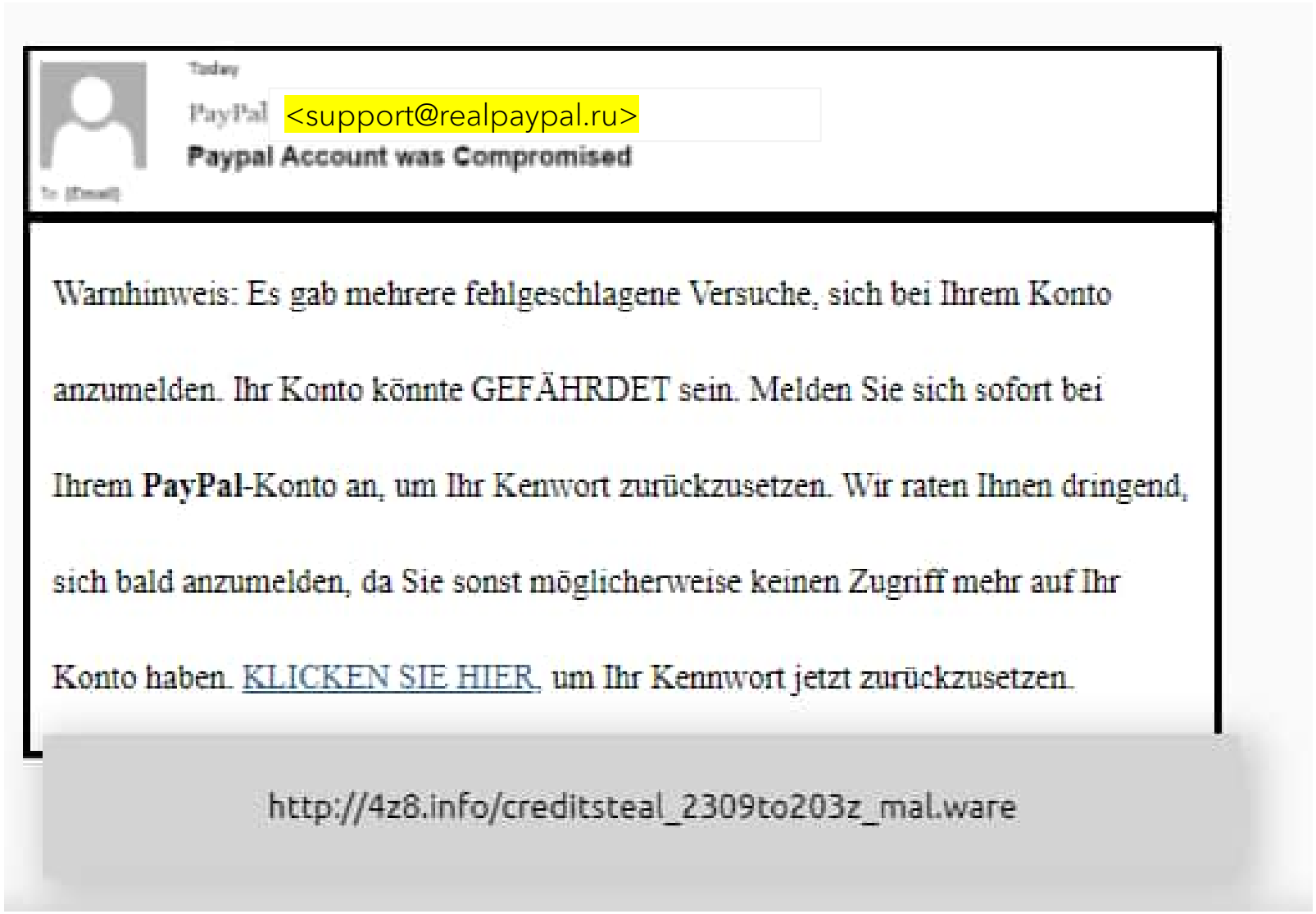
Step 1 Protect yourself using 1Password to generate and save strong passwords for each website.

Step 2 Enable 2 factor authentication and store the codes inside your 1Password account.

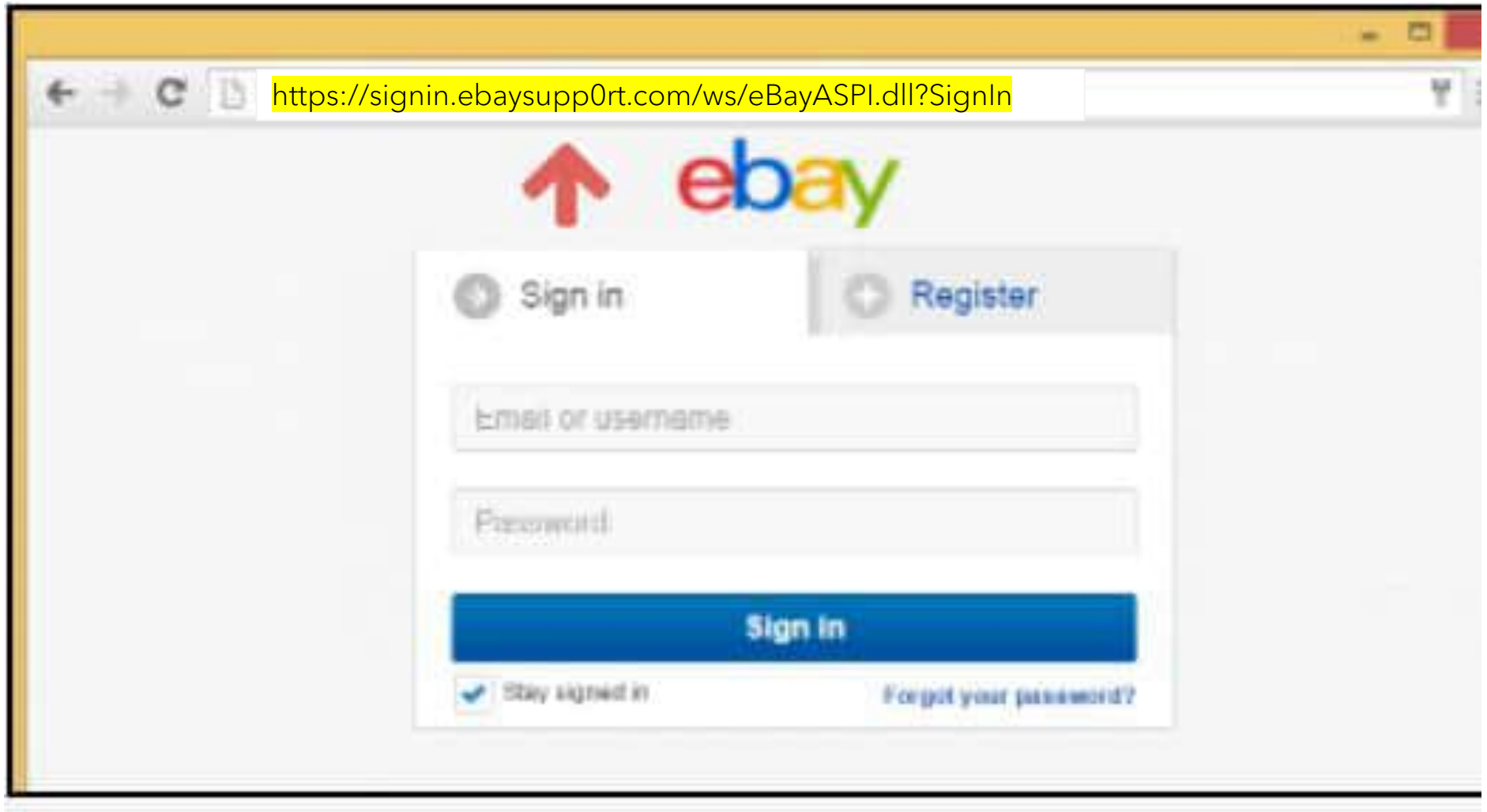
Step 3 Subscribe to notifications for any other breaches. Then just change that unique password.



CDS
BAUSOFTWARE
BAUINGENIEURE
NETCOM



CDS
BAUSOFTWARE
BAUINGENIEURE
NETCOM

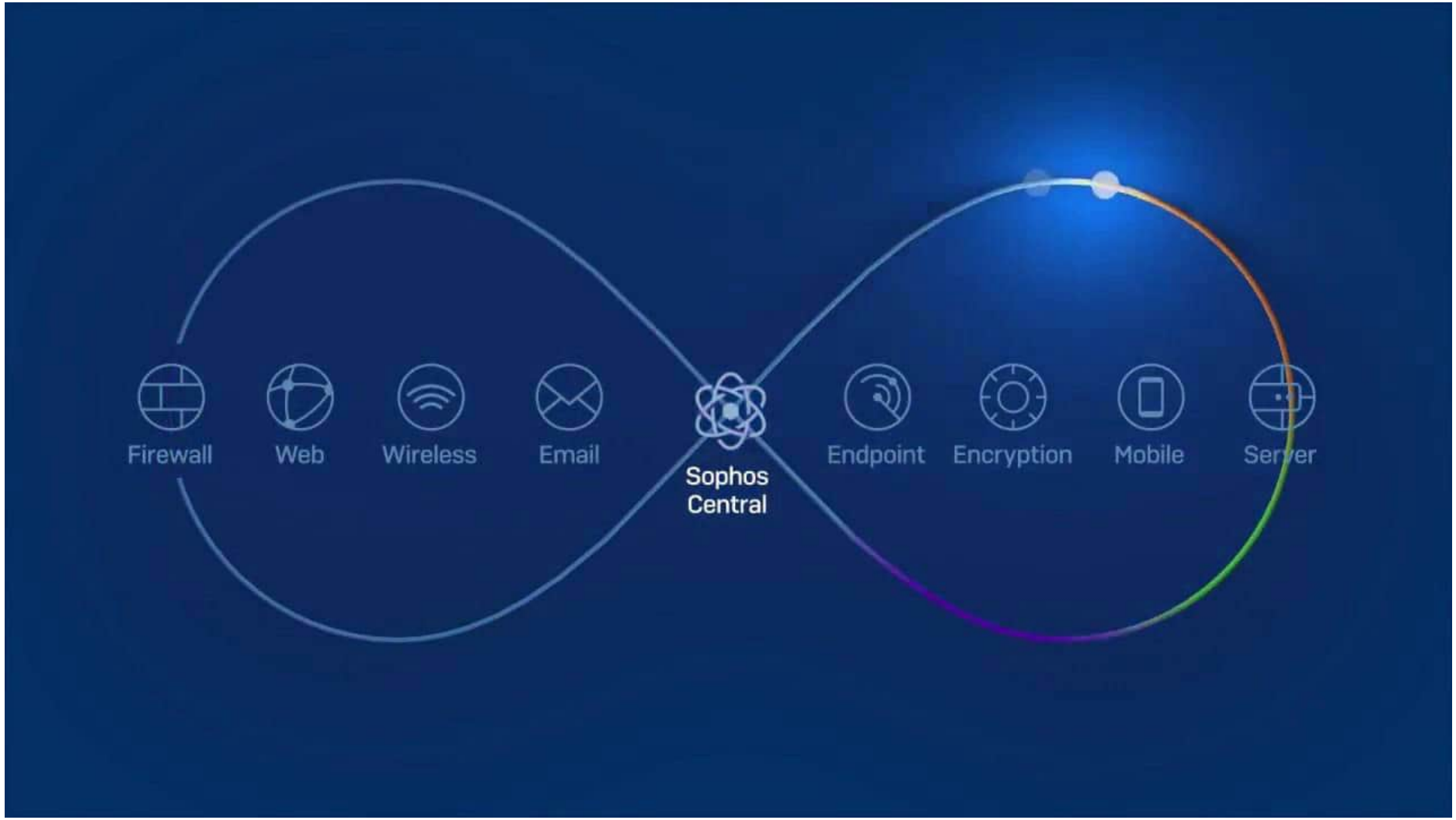


CDS
BAUSOFTWARE
BAUINGENIEURE
NETCOM

CDS
BAUSOFTWARE
BAUINGENIEURE
NETCOM

Was kommt noch dazu?

CDS
BAUSOFTWARE
BAUINGENIEURE
NETCOM



CDS
BAUSOFTWARE
BAUINGENIEURE
NETCOM


Papierkorb
Dokumente
Acrobat Reader DC
Vertraulich
Google Chrome
Microsoft Word
Microsoft Outlook
prog
INTERCEPT X
DEU
14:47
03.03.2017

Zu guter Letzt?

CDS
BAUSOFTWARE
BAUINGENIEURE
NETCOM

Wenn eine befallene E-Mail an 100 Personen geschickt wird …

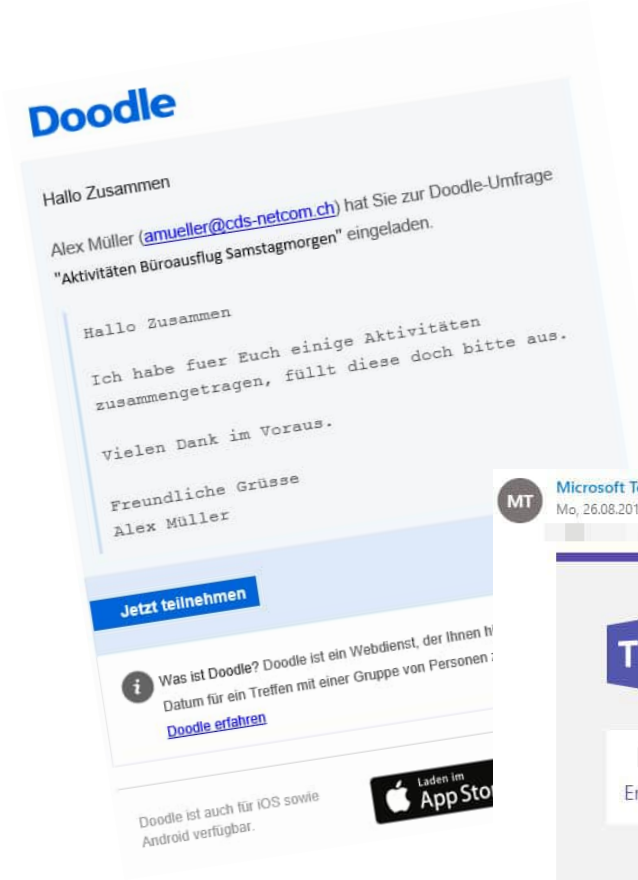
…. werden 30 Personen die E-Mail öffnen …

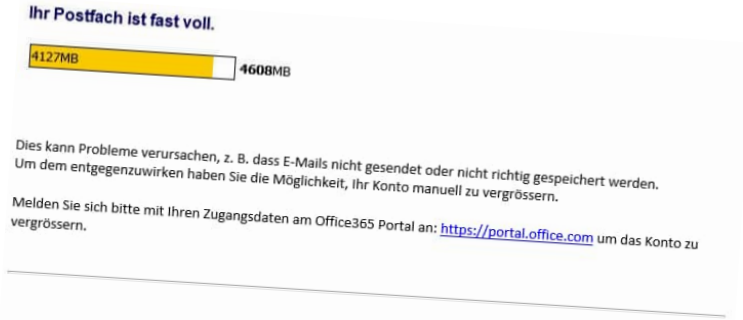
…. und 12 Personen werden den Anhang öffnen….

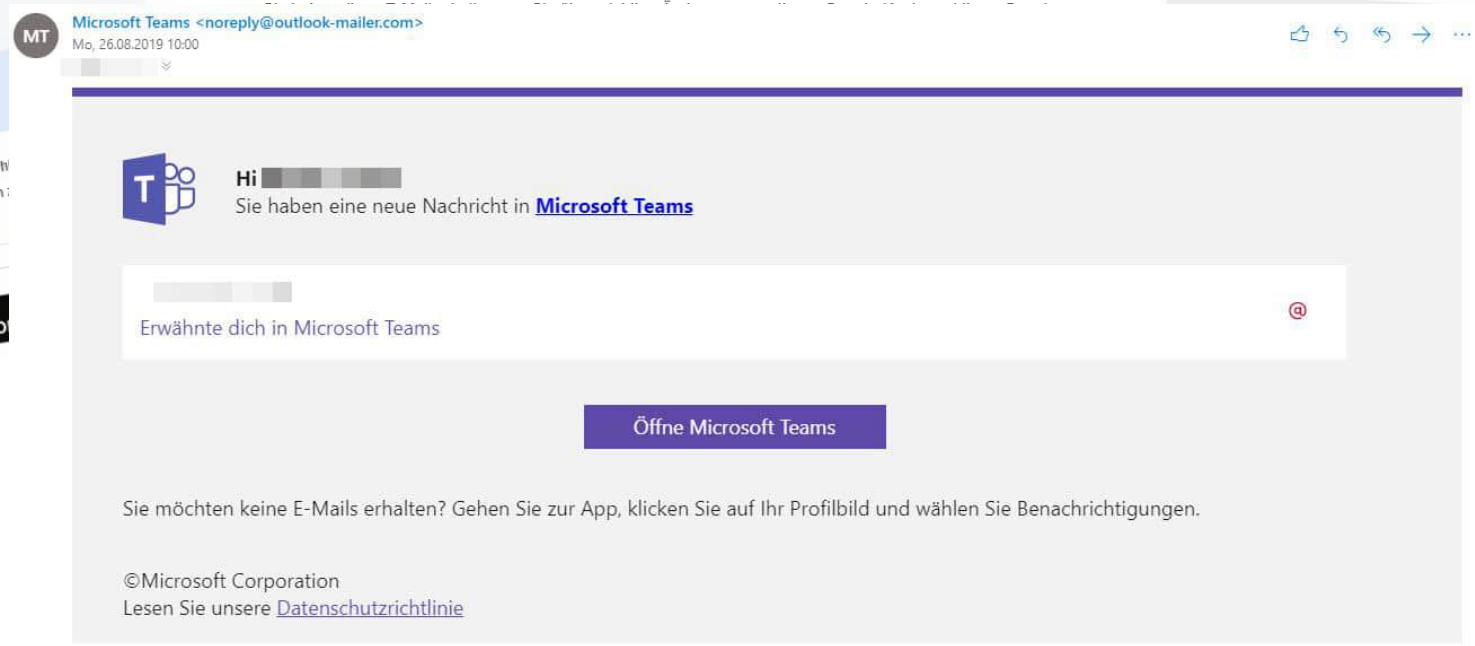
…. und das innerhalb von 3 Minuten und 45 Sekunden.

66 % der heutigen Schadsoftware wird durch befallene E-Mails verteilt.

CDS
BAUSOFTWARE
BAUINGENIEURE
NETCOM







CDS
BAUSOFTWARE
BAUINGENIEURE
NETCOM

CDS

BAUSOFTWARE
BAUINGENIEURE
NETCOM

Exkursion ins „dunkle Internet“

CDS
BAUSOFTWARE
BAUINGENIEURE
NETCOM

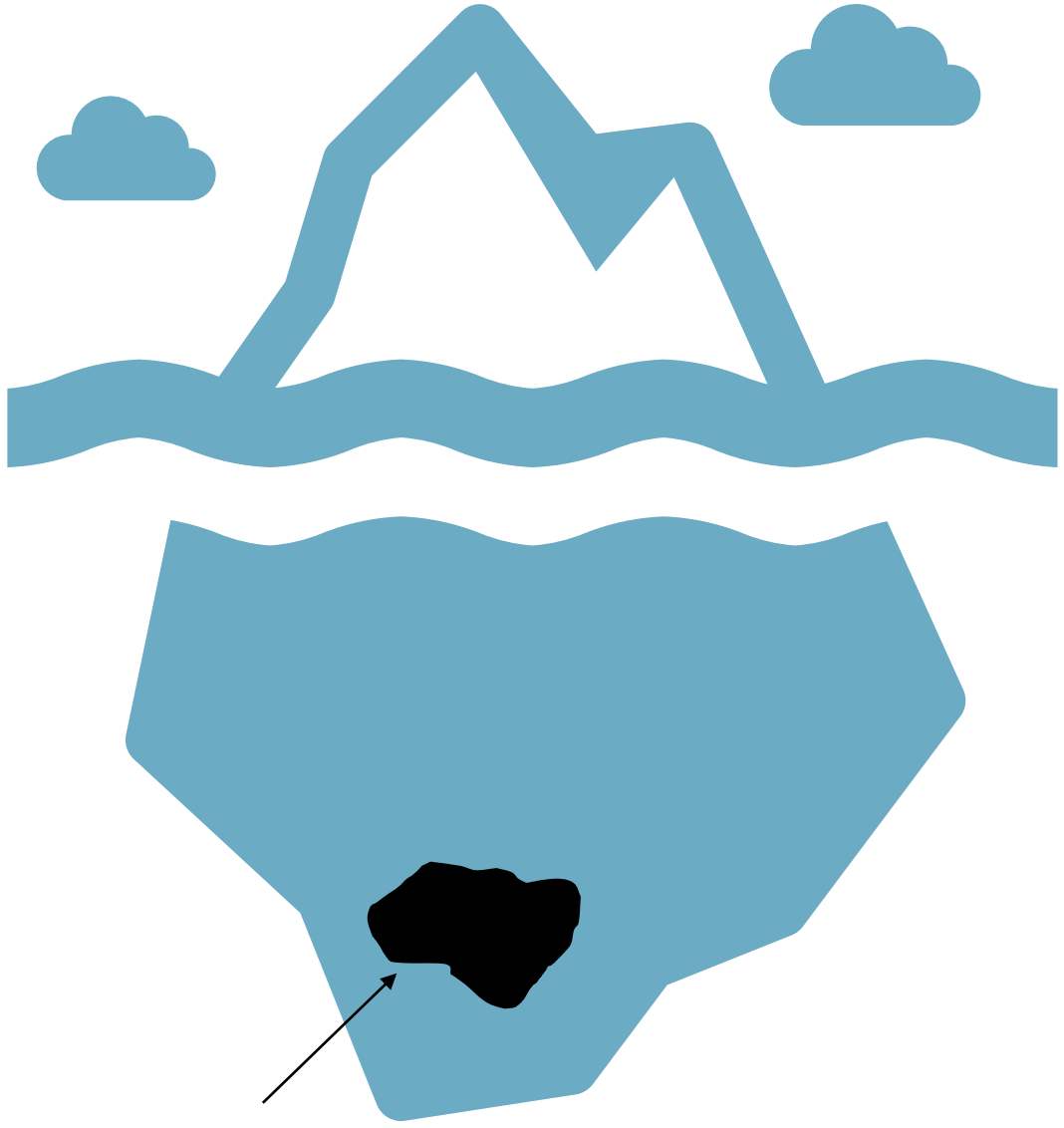
Clear Web

CDS
BAUSOFTWARE
BAUINGENIEURE
NETCOM

Clear Web

Deep Web

CDS
BAUSOFTWARE
BAUINGENIEURE
NETCOM



Clear Web

Deep Web

Darknet

CDS
BAUSOFTWARE
BAUINGENIEURE
NETCOM

CDS
BAUSOFTWARE
BAUINGENIEURE
NETCOM

CDS
BAUSOFTWARE
BAUINGENIEURE
NETCOM