



IT Security in Zahnarztpraxen

Wenn Würmer, Viren und Trojaner die Patientendossiers zerstören!

Vorstellung



Marco Dornig

Stv. Leiter CDS Netcom

Beratung von KMU's

Agenda

Einstieg

Bedrohungen

Wie können wir uns schützen?

Exkursion ins «dunkle» Internet

Fragen?

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](#)

Jahresvergleich von Check Point 11.01.2022, 08:04 Uhr

65 Prozent mehr Cyberangriffe in der Schweiz

Trauriger Rekord: Hafnium-Angriffe auf Server betreffen

Wohl seit Wochen greift die chinesische Gruppe über eine Schwachstelle an. Nun gibt es



Es werden Hackerangriffe auf



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.

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

INCIDENTS

06 JUN 2022

2 minute read



AUTHORS

Expert 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](#).

Studie: Über 3000 Schweizer Unternehmen haben bereits Kundendaten verloren

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

SECURITY

PHISHING

SCAMVIRUS

DATENSCHUTZ

DIGITALSWITZERLAND

VERBAN

Log4Shell-Lücke: Das sagen die Entwickler von Log4j

17.12.2021, 17:39

INTERNATIONAL DEVELOPER OPEN SOURCE APACHE



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](#)

mutmasslich einen zweiten Teil veröffentlicht. Sie wollen ein Lösegeld erpressen. 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?



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!

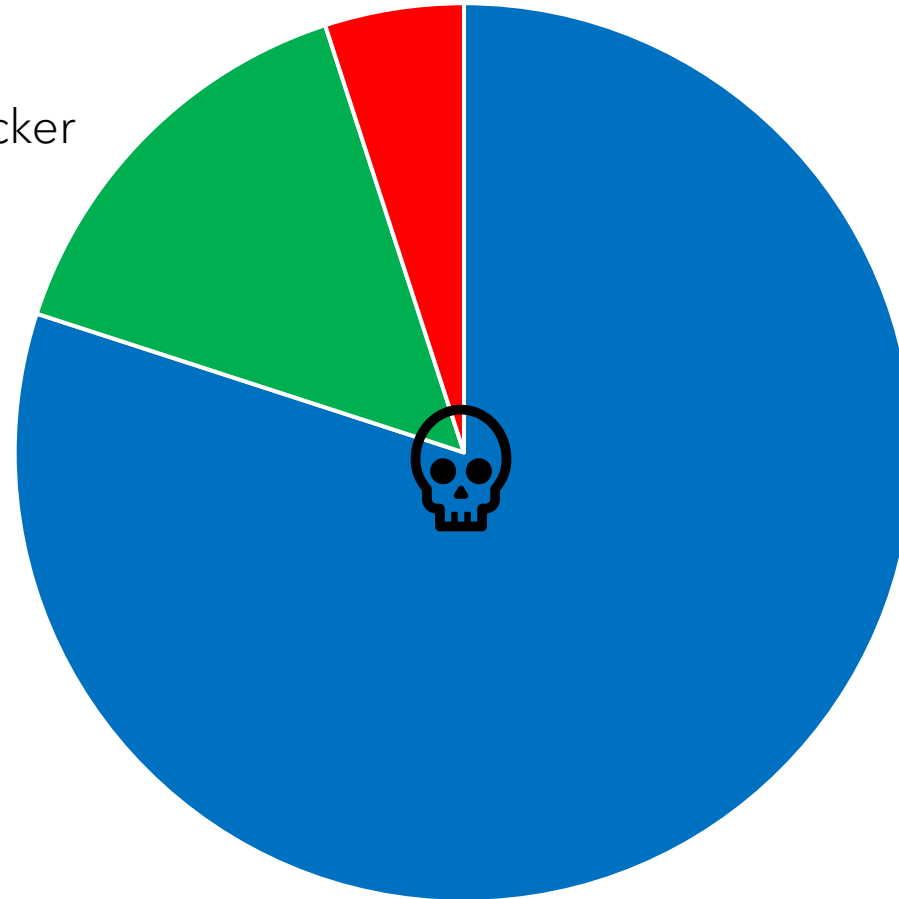
Firewall und AntiVirus reichten schon immer!

Bedrohungen verändern sich!

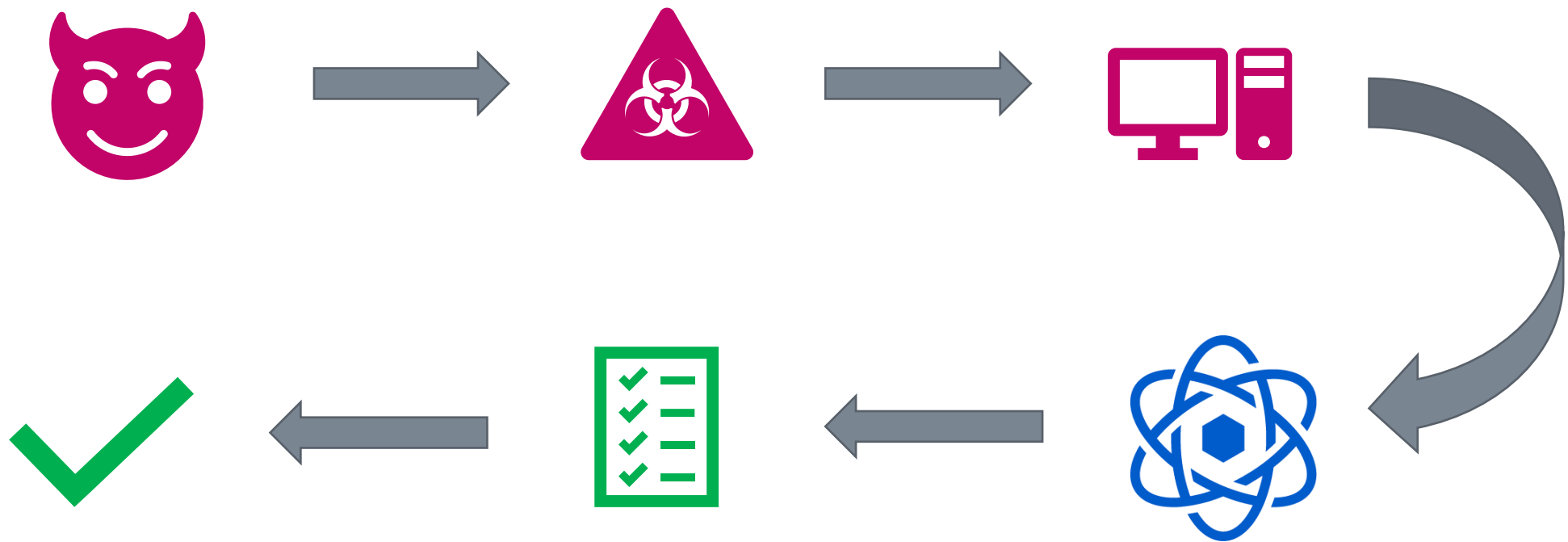
Bedroher von vor 20 Jahren

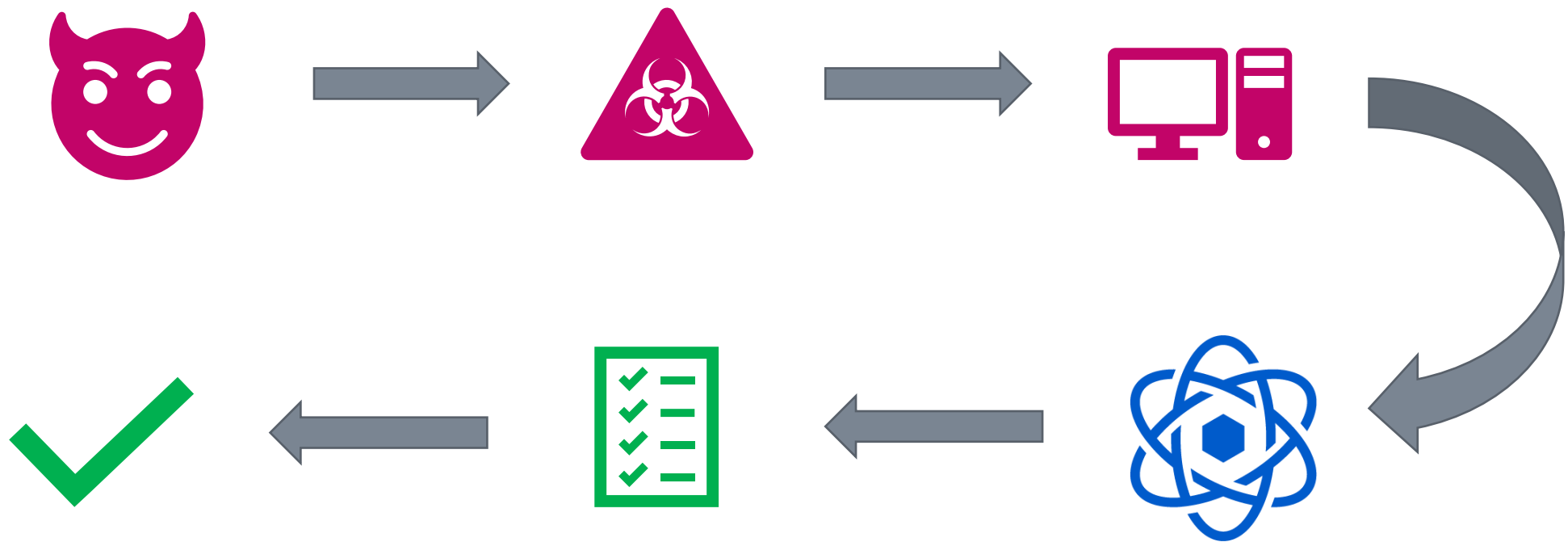
Moderne Angreifer

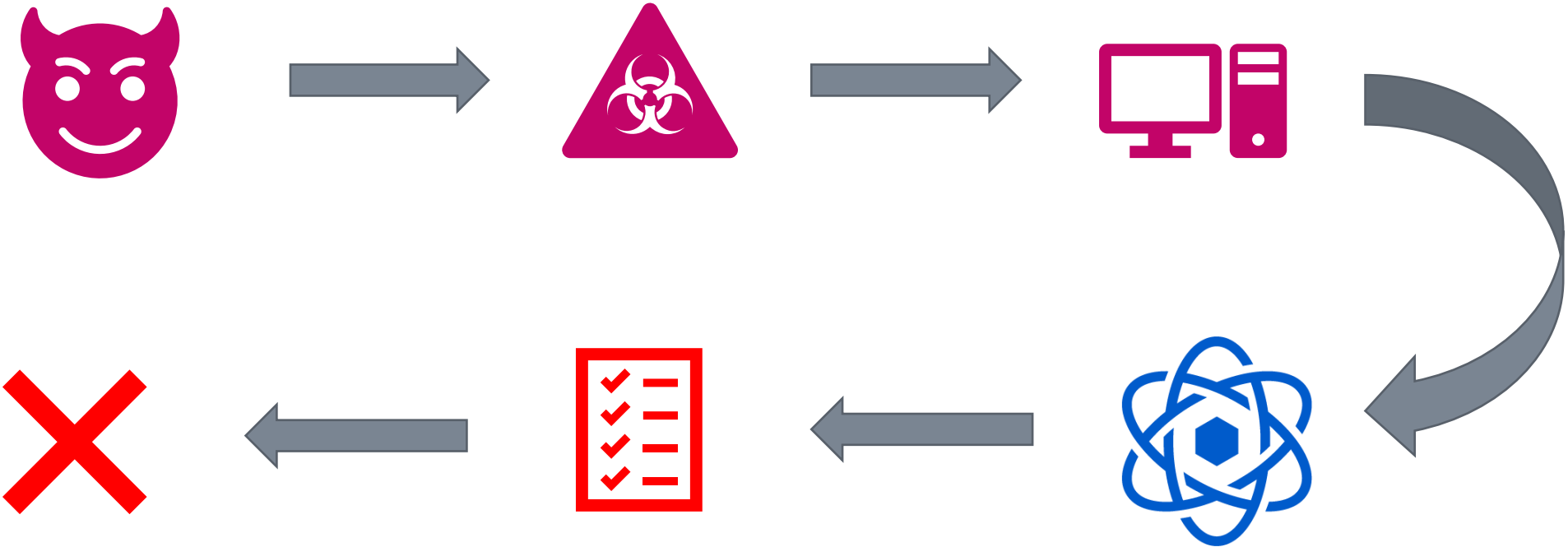
Hacker



Skript Kiddies aus den 2000ern.



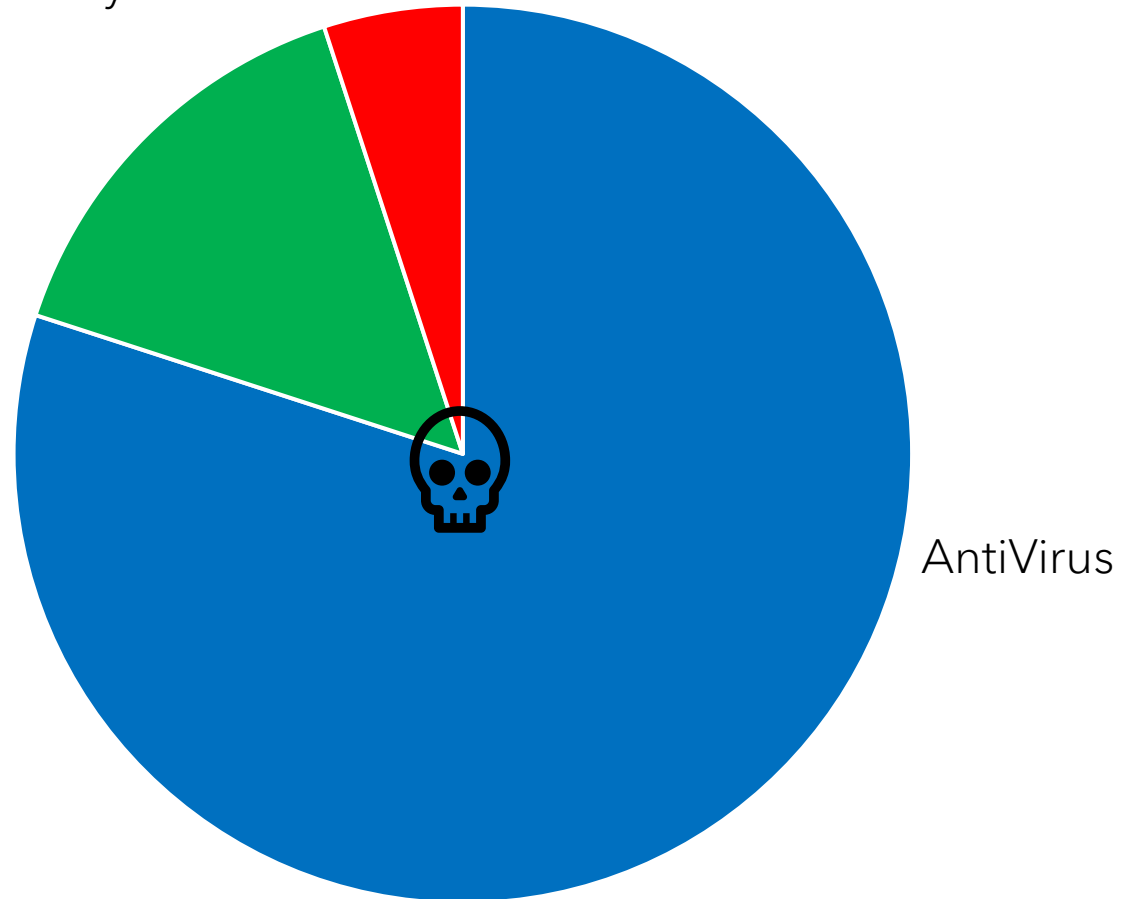






Was nützte gegen diese Bedrohungen

KnowHow im Securitybereich



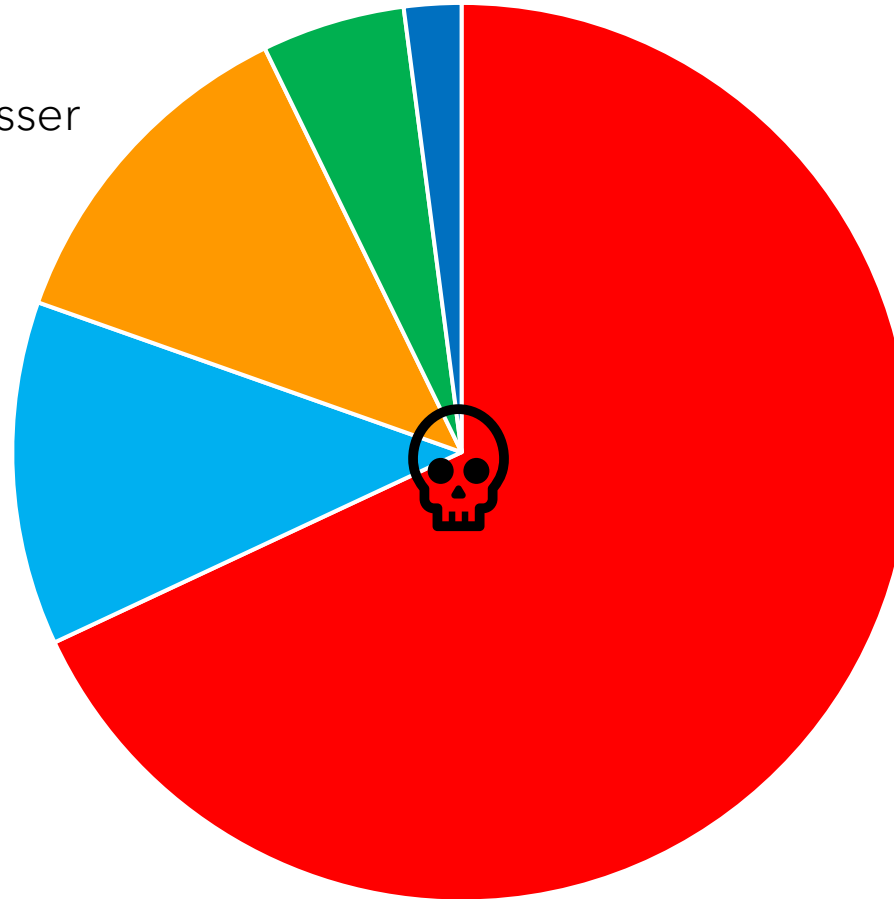
Bedroher von Heute

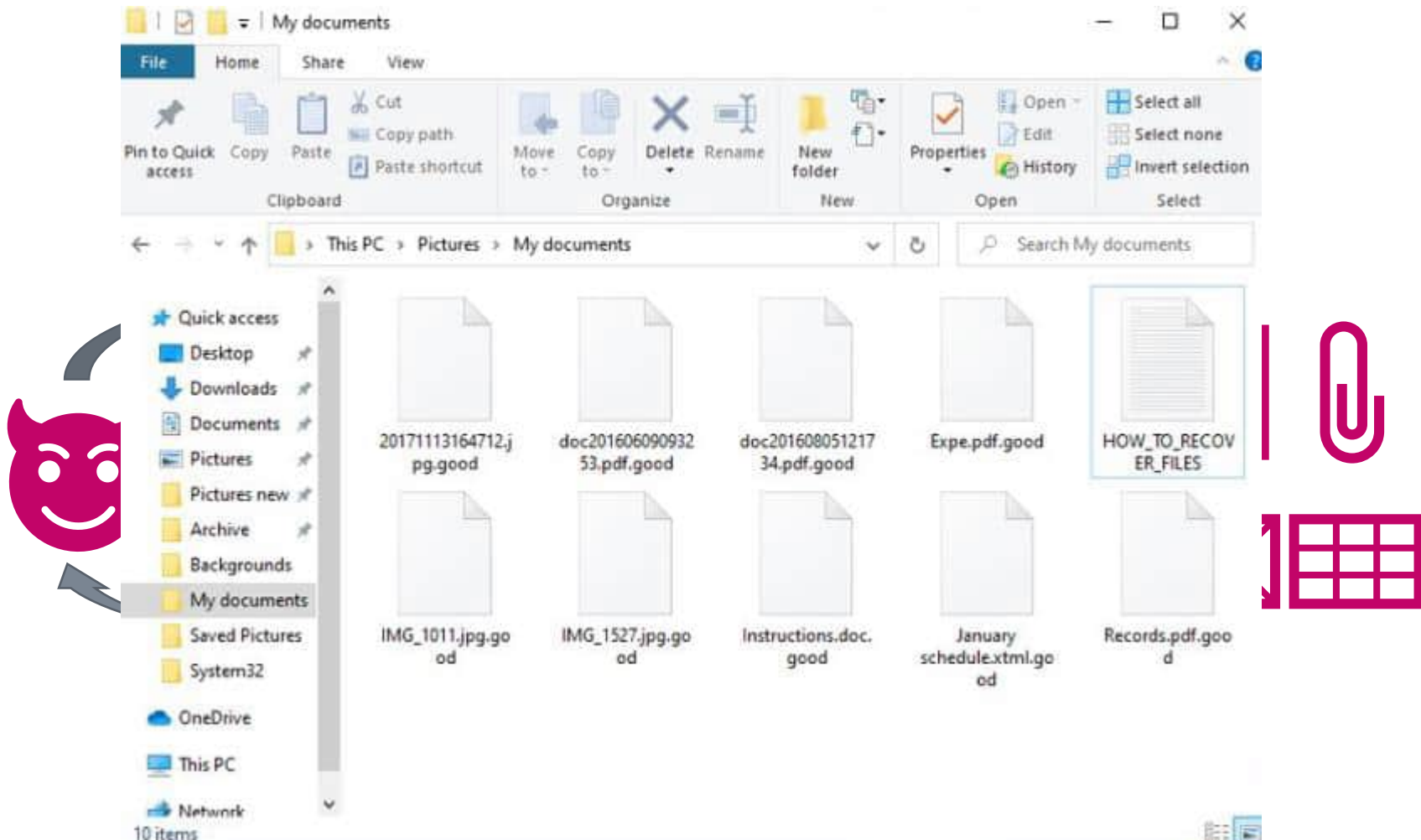
Hacker Skript Kiddies aus den 2000ern

Erpresser

Strom-Diebe

Moderne Angreifer





cmdroot@airmail.cc



All your files have been encrypted!

All your files have been encrypted due to a security problem with your PC. If you want to restore them, write us to the e-mail cmdroot@airmail.cc

Write this ID in the title of your message **1E857D00**

In case of no answer in 24 hours write us to these e-mails: cmdroot@airmail.cc

You have to pay for decryption in Bitcoins. The price depends on how fast you write to us. After payment we will send you the decryption tool that will decrypt all your files.

Free decryption as guarantee

Before paying you can send us up to 1 file for free decryption. The total size of files must be less than 1Mb (non archived), and files should not contain valuable information. (databases, backups, large excel sheets, etc.)

How to obtain Bitcoins

The easiest way to buy bitcoins is LocalBitcoins site. You have to register, click 'Buy bitcoins', and select the seller by payment method and price.

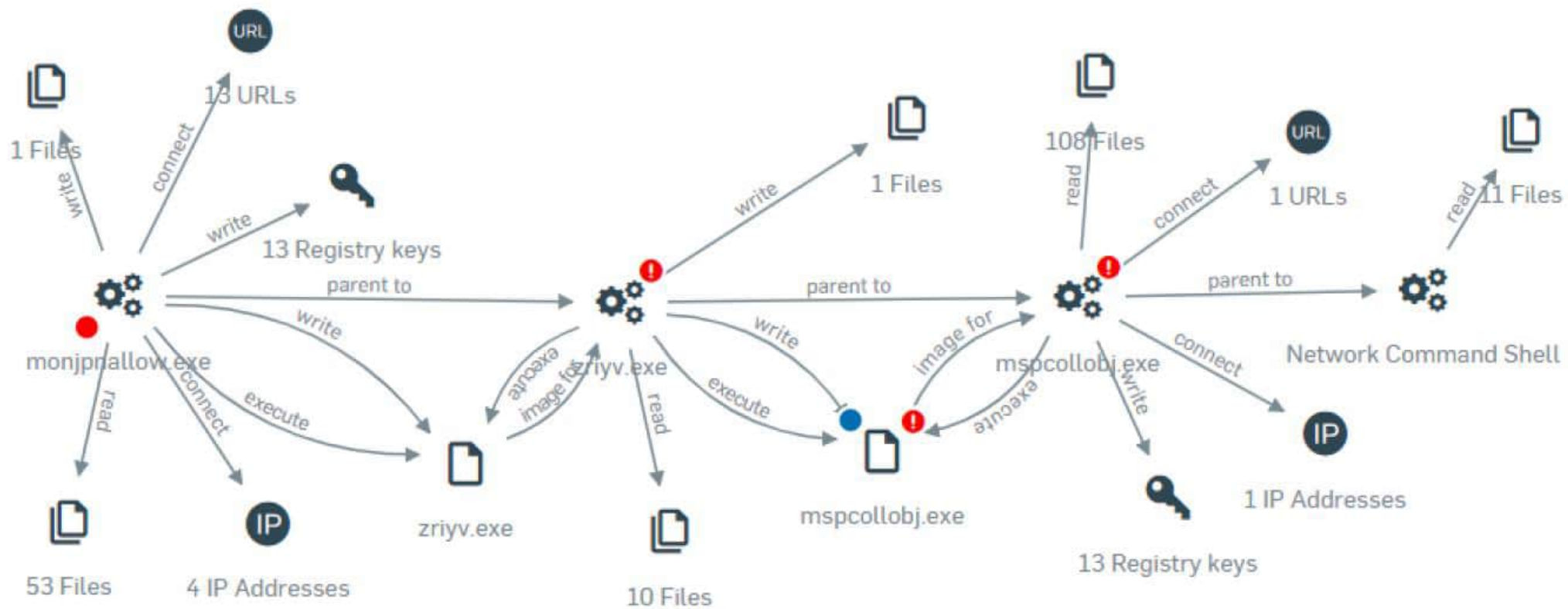
<https://localbitcoins.com/buy-bitcoins>

Also you can find other places to buy Bitcoins and beginners guide here:

<http://www.comdesk.com/information/how-can-i-buy-bitcoins/>

Attention!

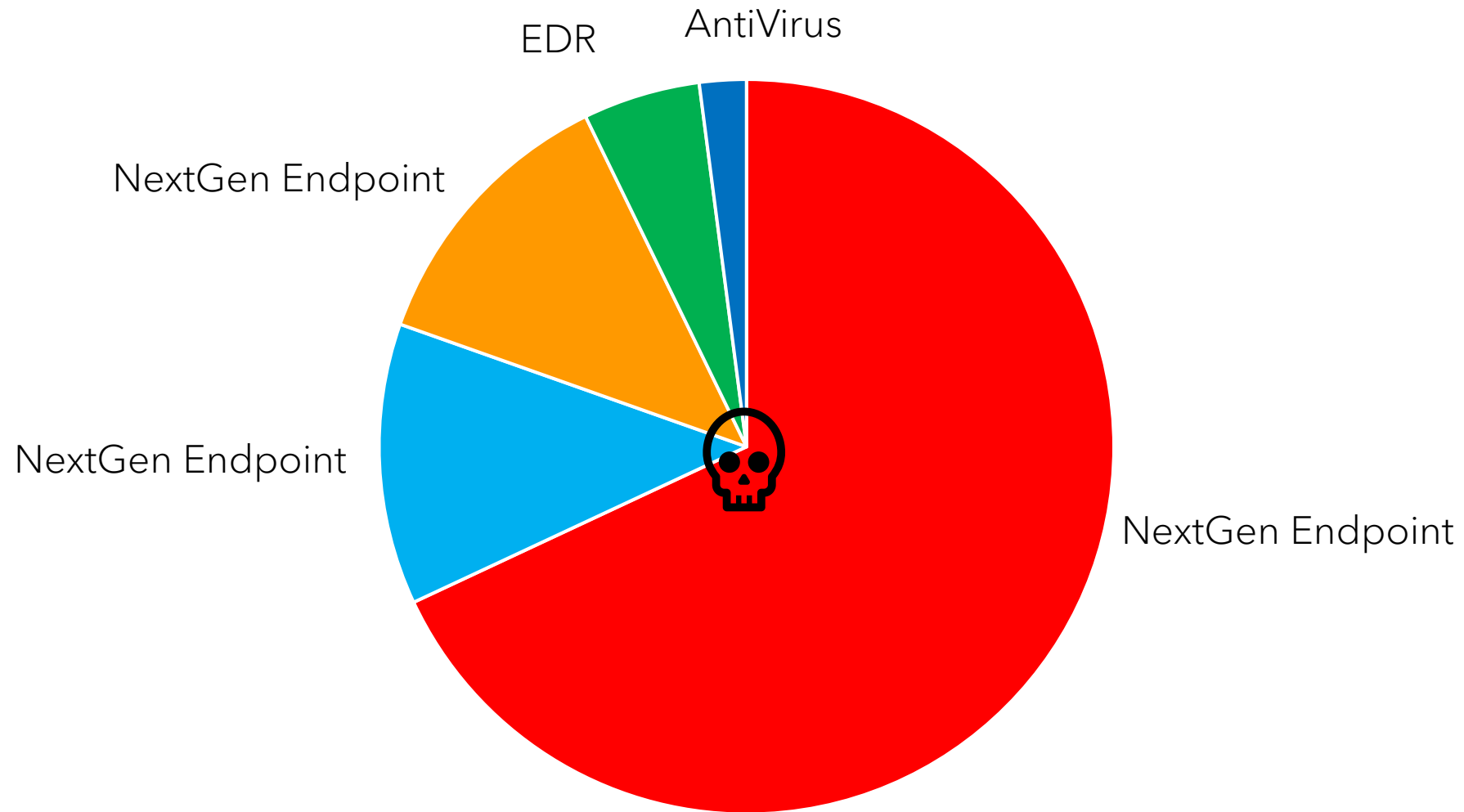
- Do not rename encrypted files.
- Do not try to decrypt your data using third party software, it may cause permanent data loss.
- Decryption of your files with the help of third parties may cause increased price (they add their fee to our) or you can become a victim of a scam.



- 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?



Wie können Sie sich einfach schützen?

123456
password
12345678
12341234
1asdadasdasd
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



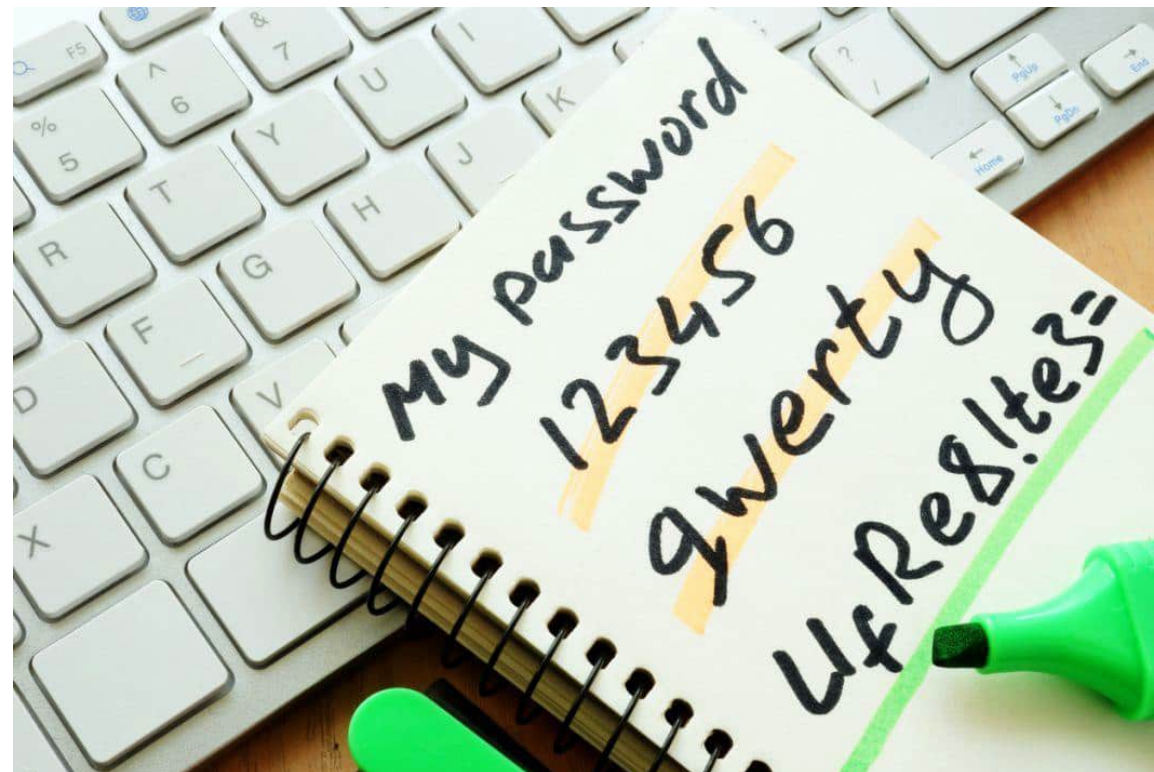
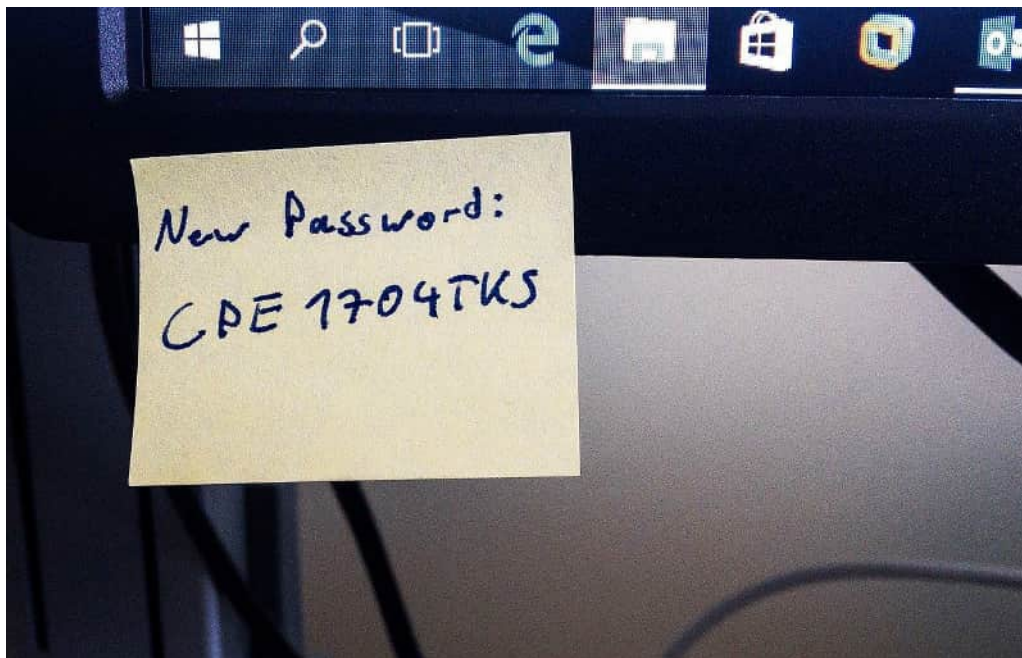
Step 1 Protect yourself using 1Password to generate and save strong passwords for each website.



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.





Today

PayPal

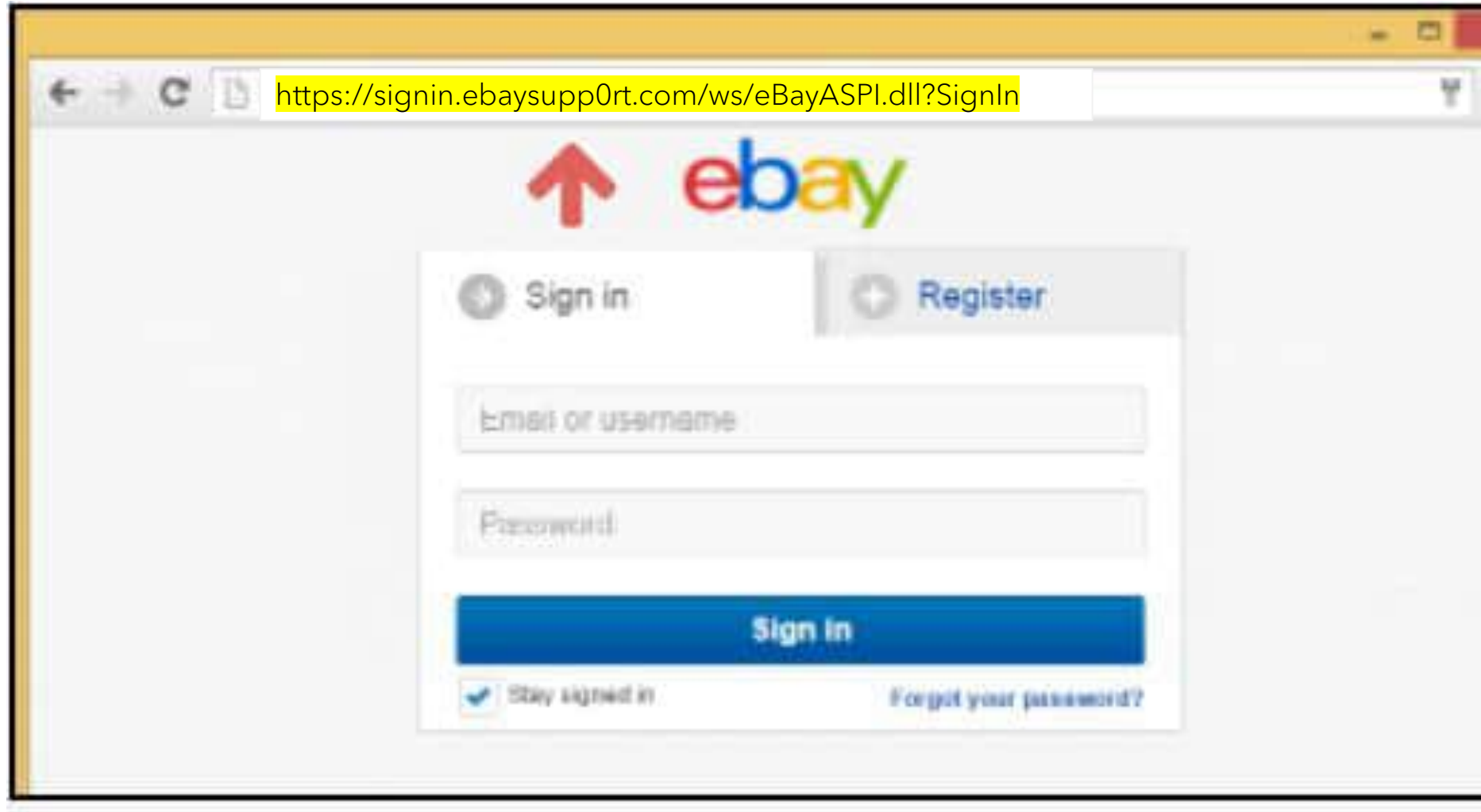
<support@realpaypal.ru>

Paypal Account was Compromised

To: (Email)

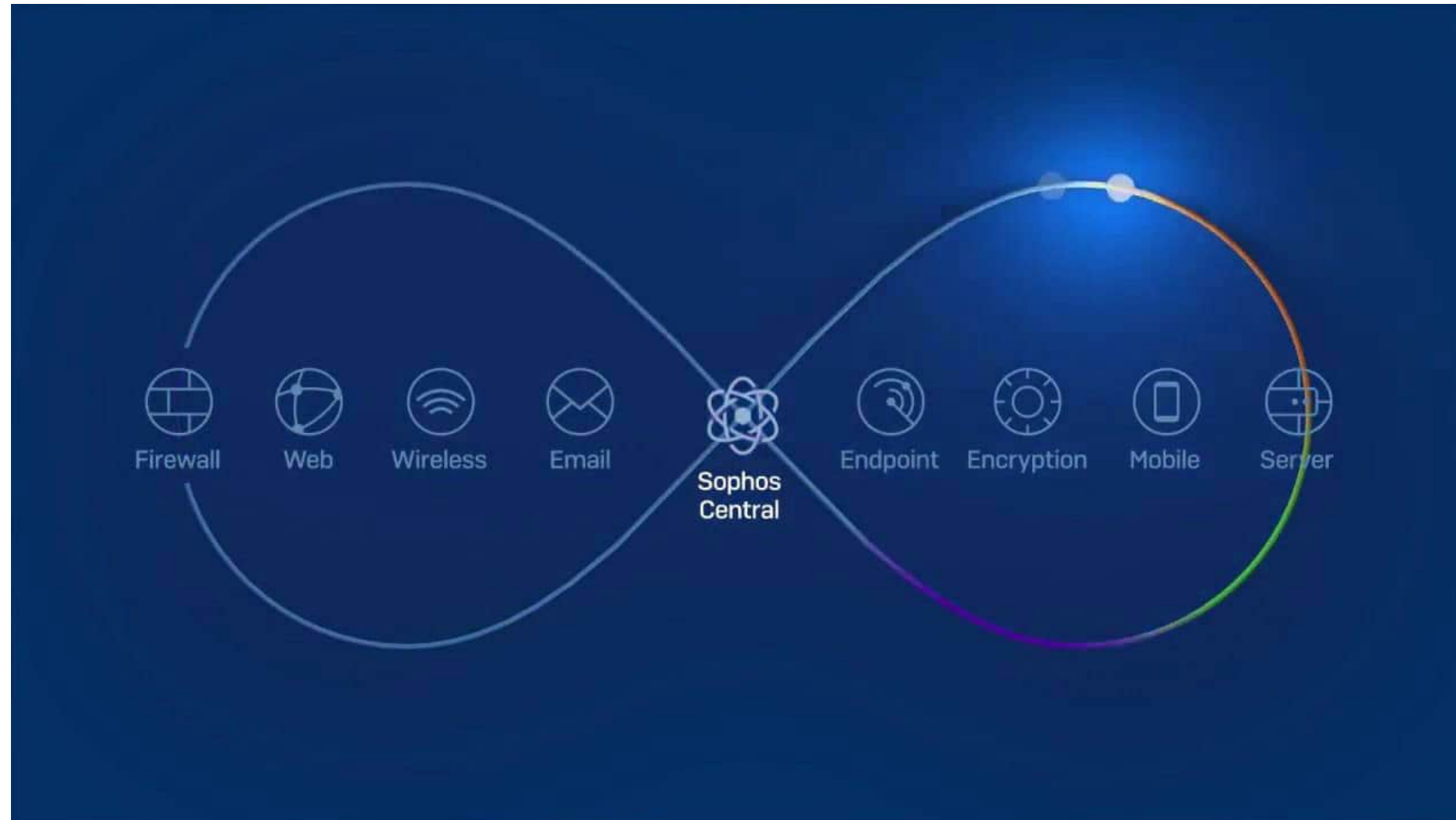
Warnhinweis: Es gab mehrere fehlgeschlagene Versuche, sich bei Ihrem Konto anzumelden. Ihr Konto könnte GEFÄHRDET sein. Melden Sie sich sofort bei Ihrem PayPal-Konto an, um Ihr Kennwort zurückzusetzen. Wir raten Ihnen dringend, sich bald anzumelden, da Sie sonst möglicherweise keinen Zugriff mehr auf Ihr Konto haben. [KLICKEN SIE HIER](http://4z8.info/creditsteal_2309to203z_mal.ware), um Ihr Kennwort jetzt zurückzusetzen.

http://4z8.info/creditsteal_2309to203z_mal.ware





Was kommt noch dazu?





Papierkorb



Dokumente



Acrobat Reader DC



Vertraulich



Google Chrome



Microsoft Word



Microsoft Outlook



prog

INTERCEPT



14:47
03.03.2017

Zu guter Letzt?



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.

Doodle

Hallo Zusammen

Alex Müller (amueller@cds-netcom.ch) hat Sie zur Doodle-Umfrage "Aktivitäten Büroausflug Samstagmorgen" eingeladen.

Hallo Zusammen

Ich habe fuer Euch einige Aktivitäten zusammengetragen, füllt diese doch bitte aus.

Vielen Dank im Voraus.

Freundliche Grüsse
Alex Müller

Jetzt teilnehmen

Was ist Doodle? Doodle ist ein Webdienst, der Ihnen hilft, Datum für ein Treffen mit einer Gruppe von Personen zu wählen.
[Doodle erfahren](#)

Doodle ist auch für iOS sowie Android verfügbar.



Google



Anmeldeversuch wurde blockiert

Jemand hat gerade Ihr Passwort verwendet, um sich in Ihrem Konto anzumelden. Google hat sie blockiert, aber Sie sollten überprüfen, was passiert ist.

[AKTIVITÄT PRÜFEN](#)

Ihr Postfach ist fast voll.

4127MB 4608MB

Dies kann Probleme verursachen, z. B. dass E-Mails nicht gesendet oder nicht richtig gespeichert werden. Um dem entgegenzuwirken haben Sie die Möglichkeit, Ihr Konto manuell zu vergrößern.

Melden Sie sich bitte mit Ihren Zugangsdaten am Office365 Portal an: <https://portal.office.com> um das Konto zu vergrößern.

MT Microsoft Teams <noreply@outlook-mailer.com>
Mo, 26.08.2019 10:00



Hi [Name]

Sie haben eine neue Nachricht in [Microsoft Teams](#)

Erwähnte dich in Microsoft Teams

[Öffne Microsoft Teams](#)

Sie möchten keine E-Mails erhalten? Gehen Sie zur App, klicken Sie auf Ihr Profilbild und wählen Sie Benachrichtigungen.

©Microsoft Corporation
Lesen Sie unsere [Datenschutzrichtlinie](#)



#MSO365



CDS

BAUSOFTWARE
BAUINGENIEURE
NETCOM

Exkursion ins „dunkle Internet“



Clear Web



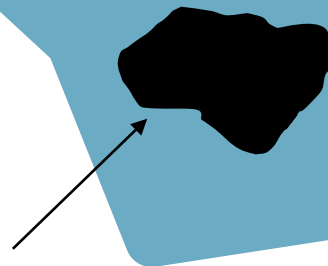
Clear Web

Deep Web



Clear Web

Deep Web



Darknet

DEMO



CDS

BAUSOFTWARE
BAUINGENIEURE
NETCOM

