POLIZEI
Nordrhein-Westfalen
Landeskriminalamt

bürgerorientiert · professionell · rechtsstaatlich

Cybercrime - aus dem Nähkästchen erzählt

SWS COMPUTERSYSTEME
Member of ACP Group

Security Forum, 29.04.2021

POLIZEI
Nordrhein-Westfalen
Landeskriminalamt

Peter Vahrenhorst

Kriminalhauptkommissar

Landeskriminalamt NRW

SG 41.1 – Cybercrime-Kompetenzzentrum

Tel.: 0211 939 4114

Fax: 0211 939 19 4114

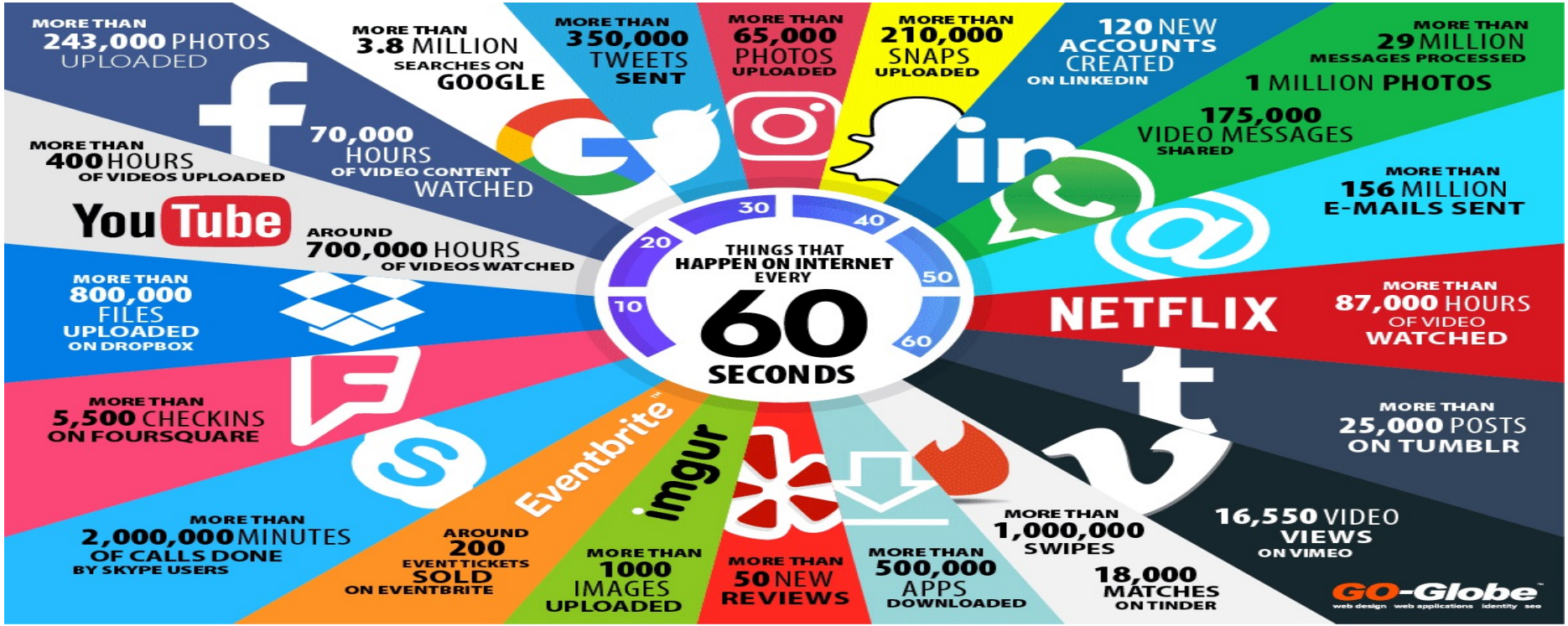
Peter.Vahrenhorst@polizei.nrw.de

SWS COMPUTERSYSTEME
Member of ACP Group

POLIZEI
Nordrhein-Westfalen
Landeskriminalamt

Herausforderung Cybercrime

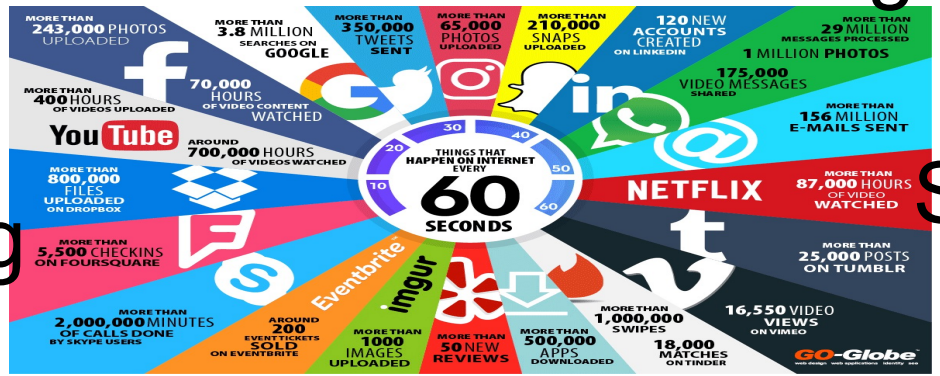
SWS COMPUTERSYSTEME
Member of ACP Group


MORE THAN 243,000 PHOTOS UPLOADED
MORE THAN 3.8 MILLION SEARCHES ON GOOGLE
MORE THAN 350,000 TWEETS SENT
MORE THAN 65,000 PHOTOS UPLOADED
MORE THAN 210,000 SNAPS UPLOADED
120 NEW ACCOUNTS CREATED ON LINKEDIN
MORE THAN 29 MILLION MESSAGES PROCESSED
1 MILLION PHOTOS
175,000 VIDEO MESSAGES SHARED
70,000 HOURS OF VIDEO CONTENT WATCHED
MORE THAN 400 HOURS OF VIDEOS UPLOADED
YouTube
AROUND 700,000 HOURS OF VIDEOS WATCHED
MORE THAN 156 MILLION E-MAILS SENT
MORE THAN 800,000 FILES UPLOADED ON DROPBOX
THINGS THAT HAPPEN ON INTERNET EVERY 60 SECONDS
NETFLIX
MORE THAN 87,000 HOURS OF VIDEO WATCHED
MORE THAN 5,500 CHECKINS ON FOURSQUARE
MORE THAN 25,000 POSTS ON TUMBLR
MORE THAN 2,000,000 MINUTES OF CALLS DONE BY SKYPE USERS
AROUND 200 EVENT TICKETS SOLD ON EVENTBRITE
MORE THAN 1000 IMAGES UPLOADED
MORE THAN 50 NEW REVIEWS
MORE THAN 500,000 APPS DOWNLOADED
MORE THAN 1,000,000 SWIPES
18,000 MATCHES ON TINDER
16,550 VIDEO VIEWS ON VIMEO
GO-Globe
web design web applications identity seo

digitale Transformation

e-government

e-health



e-schooling

Smart Factory

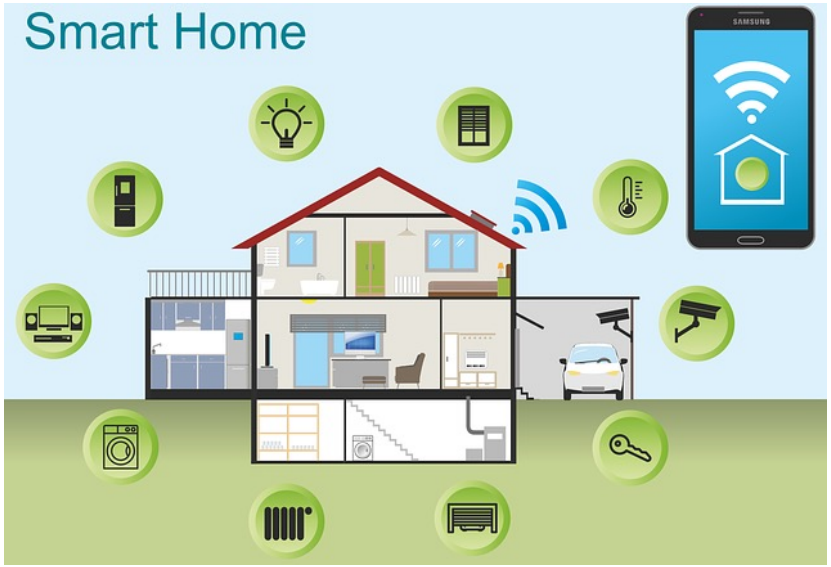
KI/AI

cloud

automotive-IT

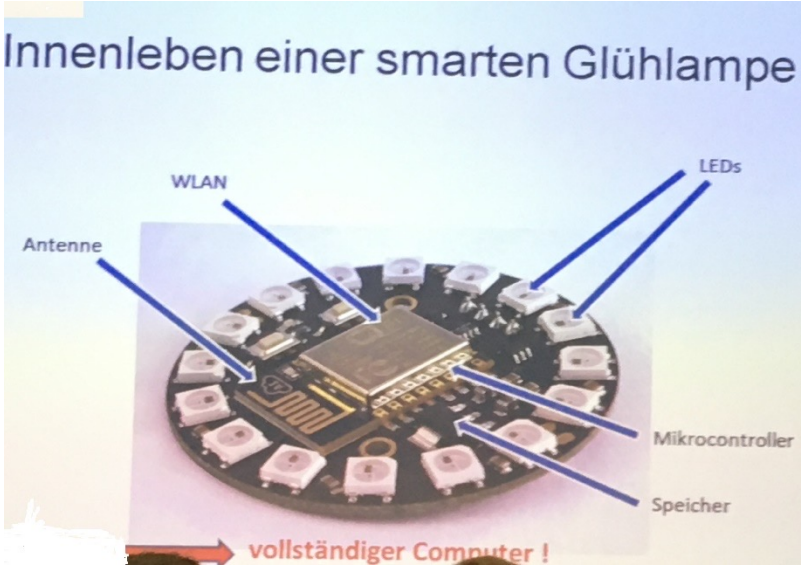
smart home


12:05
1:15Std
Wasch-automat
Start um 17:08
Dampfgarer
ein
Geschirr-spüler
5/-18°C
Kühl-Gefrier-Kombination
schließen


Smart Home
SAMSUNG

Glühbirne

POLIZEI
Nordrhein-Westfalen
Landeskriminalamt



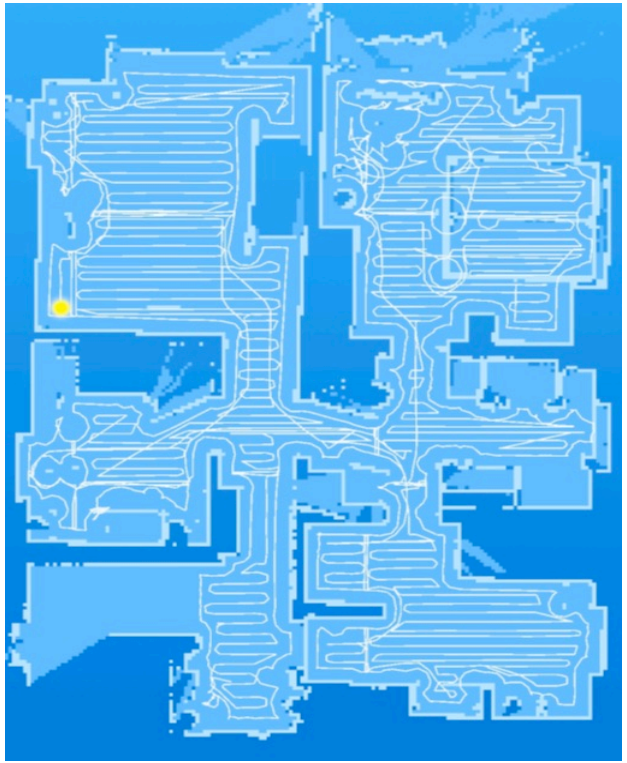
Saugroboter

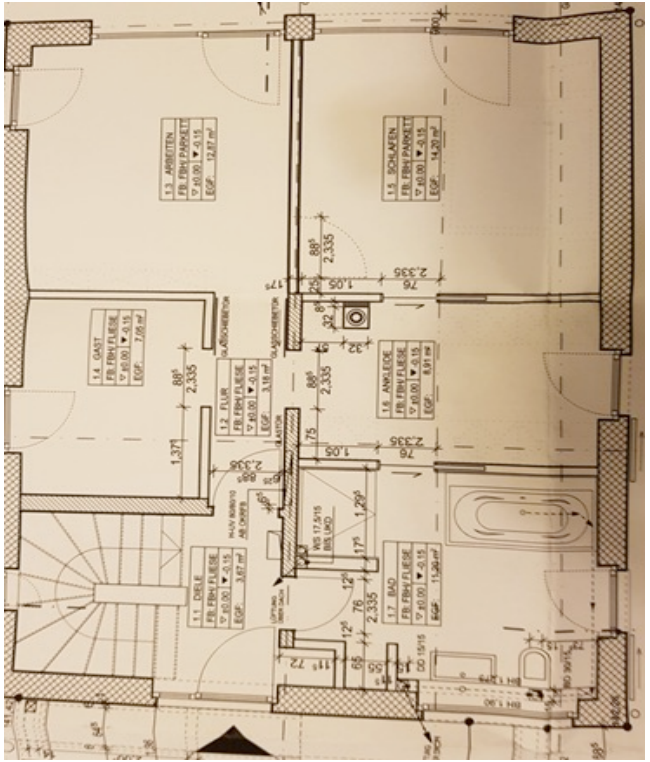
POLIZEI
Nordrhein-Westfalen
Landeskriminalamt

SWS COMPUTERSYSTEME
Member of ACP Group

Saugroboter

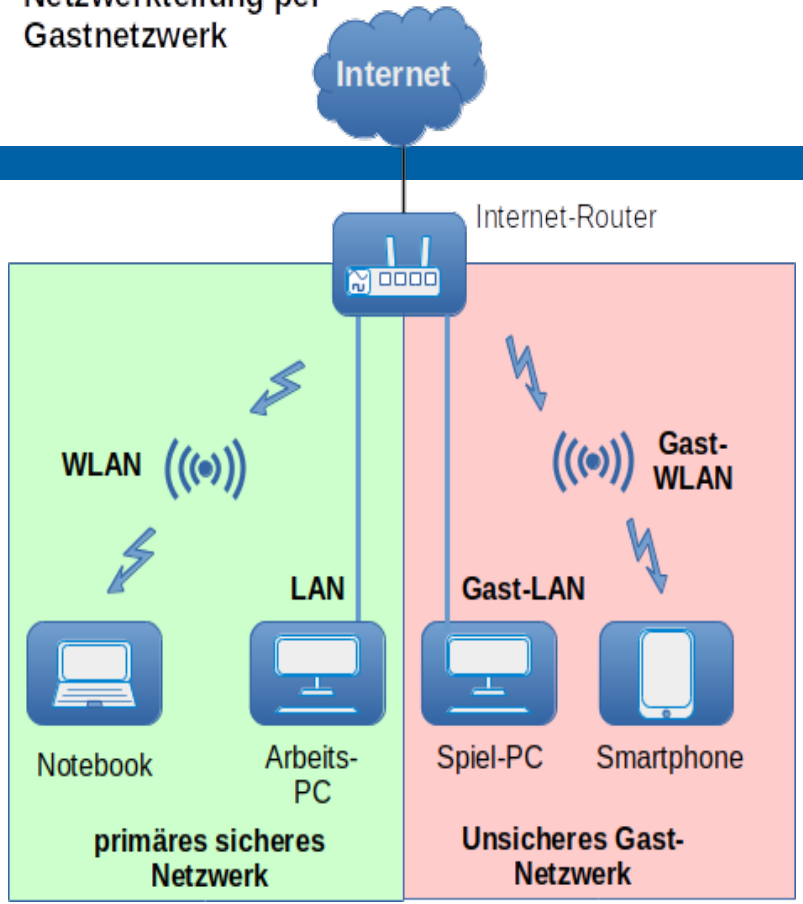
POLIZEI
Nordrhein-Westfalen
Landeskriminalamt





SWS COMPUTERSYSTEME
Member of ACP Group

Netzwerkteilung per Gastnetzwerk



POLIZEI
Nordrhein-Westfalen
Landeskriminalamt

SWS COMPUTERSYSTEME
Member of ACP Group

POLIZEI
Nordrhein-Westfalen
Landeskriminalamt

Digitalisierung vs. Corona

Umstellung

POLIZEI
Nordrhein-Westfalen
Landeskriminalamt

Schatten IT

POLIZEI
Nordrhein-Westfalen
Landeskriminalamt

Cybersecurity in Zeiten der Corona-Pandemie

Das Risiko von Cyberangriffen im Home Office reduzieren

26. März 2020

Der TÜV-Verband hat vor den Gefahren für die Cybersecurity im Zusammenhang mit dem mobilen Arbeiten im Homeoffice gewarnt. „Unternehmen müssen wegen der Corona-Pandemie die Risiken für ihre Organisation neu bewerten und ihre IT-Sicherheitsmaßnahmen anpassen“, sagte Dr. Joachim Bühler, Geschäftsführer des TÜV-Verbands (VdTÜV).

„Viele Mitarbeiter haben mit

SWS COMPUTERSYSTEME
Member of ACP Group

POLIZEI
Nordrhein-Westfalen
Landeskriminalamt

Die dunkle Seite

POLIZEI
Nordrhein-Westfalen
Landeskriminalamt

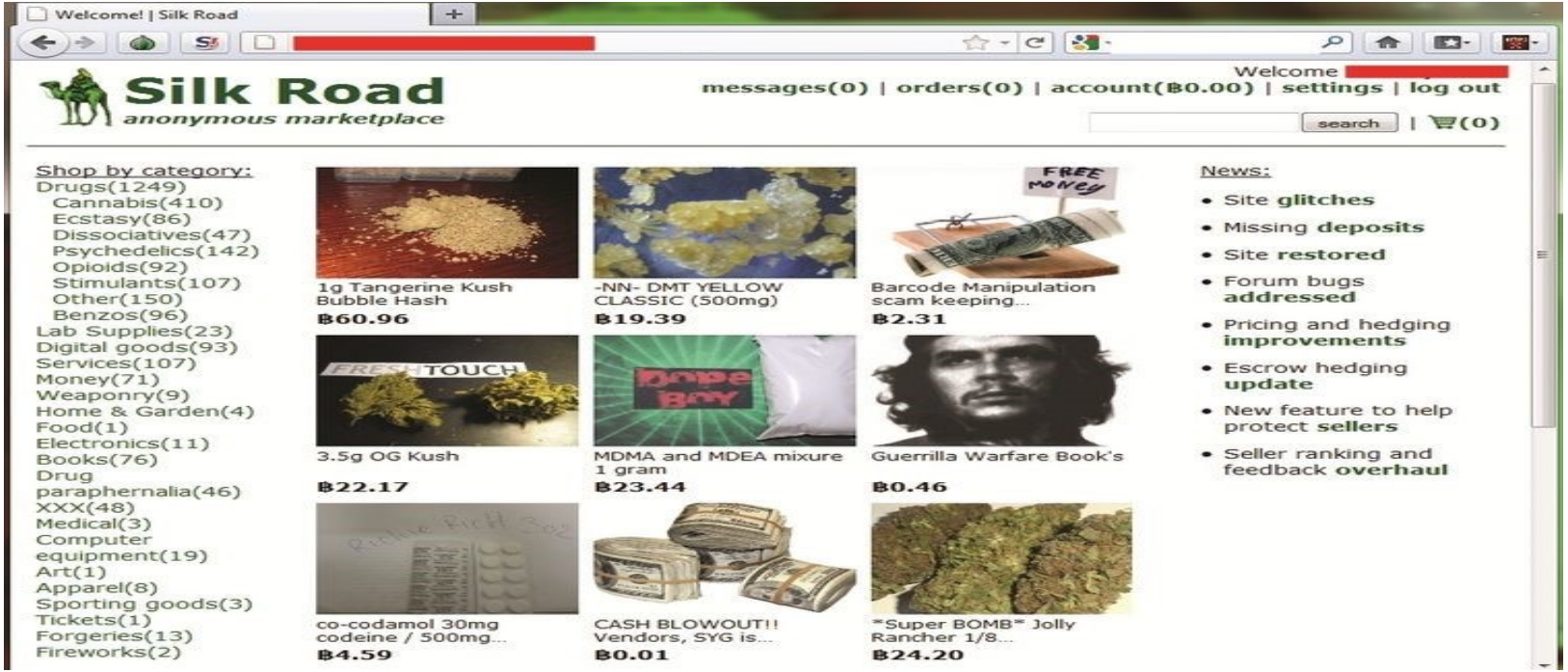
SWS COMPUTERSYSTEME
Member of ACP Group

Security Forum, 29.04.2021


Surface Web
Google
Bing
Wikipedia
Deep Web
Wissenschaftliche Studien
Enthält 90% der Informationen im Internet
Vielsprachige Datenbasis
Social Media
Rechtliche Dokumente
Illegale Informationen
Dark Web
Politische Proteste
TOR-Seiten
Teil des Deep Web, der nur über spezielle Browser erreicht werden kann und der Anonymität gewährleisten soll.
Bezugsort für Drogen
Private Kommunikation

Beispiel für „Hidden Service“

POLIZEI
Nordrhein-Westfalen
Landeskriminalamt



SWS COMPUTERSYSTEME
Member of ACP Group

POLIZEI
Nordrhein-Westfalen
Landeskriminalamt

SWS COMPUTERSYSTEME
Member of ACP Group

Natronlauge 100-fach erhöhen

09.02.2021, 07:38 Uhr

Hacker wollte Wasser in Florida verseuchen

Der Angriff auf die Aufbereitungsanlage nahe Tampa wurde noch rechtzeitig bemerkt – doch wer steckt dahinter? Das FBI und der Secret Service ermitteln.

Ein IT-Spezialist der Wasserwerke in Tampa, Florida, hat einen Cyberangriff bemerkt FOTO: GETTY IMAGES/ISTOCKPHOTO

Unbekannte stören durch "Zoom-Bombing" den Unterricht – auch in Freiburger Klasse

Von Elena Stenzel
Do, 25. Februar 2021 um 21:19 Uhr
Südwest | 2

BZ-Plus | Immer wieder dringen Unbekannte in die Programme für den Online-Unterricht ein, stören oder verbreiten extremistische Inhalte. Die Polizei ermittelt in Freiburg gegen einen sogenannten "Zoom-Bomber".

Im Normalfall läuft der Online-Unterricht ohne Störungen. Foto: vectorikart/wectorcolor (stock.adobe.com)

Systemschwachstelle

POLIZEI
Nordrhein-Westfalen
Landeskriminalamt

Was kostest „uns“ Cybercrime?

Cybercrime als Gefahr für die Wirtschaft

POLIZEI
Nordrhein-Westfalen
Landeskriminalamt

53 % betroffene Unternehmen

455.000

- Wirtschaftsspionage
- Sabotage
- Datendiebstahl

51 % haben kein Notfallmanagement

438.000

- Umsatzeinbußen
- Ausfälle
- Kundeninformation
- Imageverlust
- …

55 Milliarden €

12 Milliarden €

- Schäden im Jahr


IN CASE OF
CYBERATTACK
BREAK GLASS
AND PULL CABLES

Notfallmanagement

POLIZEI
Nordrhein-Westfalen
Landeskriminalamt

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

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.

TOP 12 MASSNAHMEN BEI CYBER-ANGRIFFEN

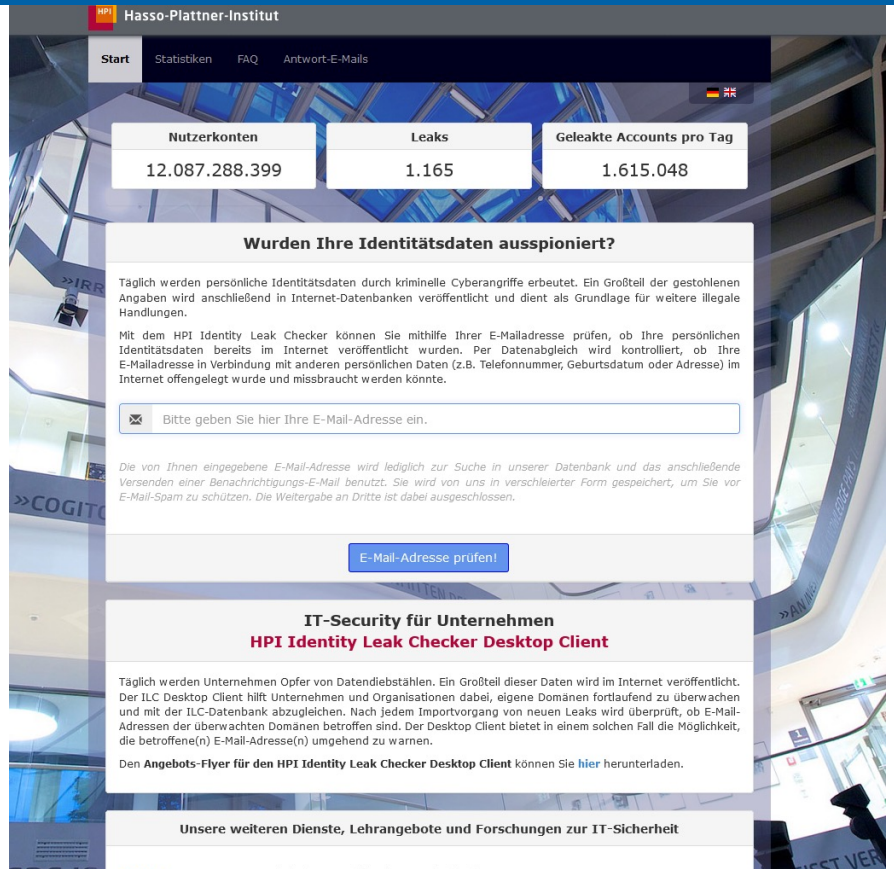
Diese Fragen sollten Sie sich stellen!

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


Hasso-Plattner-Institut
Start
Statistiken
FAQ
Antwort-E-Mails
Nutzerkonten
12.087.288.399
Leaks
1.165
Geleakte Accounts pro Tag
1.615.048
Wurden Ihre Identitätsdaten ausspioniert?
Täglich werden persönliche Identitätsdaten durch kriminelle Cyberangriffe erbeutet. Ein Großteil der gestohlenen Angaben wird anschließend in Internet-Datenbanken veröffentlicht und dient als Grundlage für weitere illegale Handlungen.
Mit dem HPI Identity Leak Checker können Sie mithilfe Ihrer E-Mailadresse prüfen, ob Ihre persönlichen Identitätsdaten bereits im Internet veröffentlicht wurden. Per Datenabgleich wird kontrolliert, ob Ihre E-Mailadresse in Verbindung mit anderen persönlichen Daten (z.B. Telefonnummer, Geburtsdatum oder Adresse) im Internet offengelegt wurde und missbraucht werden könnte.
Bitte geben Sie hier Ihre E-Mail-Adresse ein.
Die von Ihnen eingegebene E-Mail-Adresse wird lediglich zur Suche in unserer Datenbank und das anschließende Versenden einer Benachrichtigungs-E-Mail benutzt. Sie wird von uns in verschleierter Form gespeichert, um Sie vor E-Mail-Spam zu schützen. Die Weitergabe an Dritte ist dabei ausgeschlossen.
E-Mail-Adresse prüfen!
IT-Security für Unternehmen
HPI Identity Leak Checker Desktop Client
Täglich werden Unternehmen Opfer von Datendiebstählen. Ein Großteil dieser Daten wird im Internet veröffentlicht. Der ILC Desktop Client hilft Unternehmen und Organisationen dabei, eigene Domänen fortlaufend zu überwachen und mit der ILC-Datenbank abzugleichen. Nach jedem Importvorgang von neuen Leaks wird überprüft, ob E-Mail-Adressen der überwachten Domänen betroffen sind. Der Desktop Client bietet in einem solchen Fall die Möglichkeit, die betroffene(n) E-Mail-Adresse(n) umgehend zu warnen.
Den Angebots-Flyer für den HPI Identity Leak Checker Desktop Client können Sie hier herunterladen.
Unsere weiteren Dienste, Lehrangebote und Forschungen zur IT-Sicherheit

POLIZEI
Nordrhein-Westfalen
Landeskriminalamt

Was heißt das für die Polizei?

Kooperationen
Gemeinsam gegen Cybercrime

POLIZEI
Nordrhein-Westfalen
Landeskriminalamt

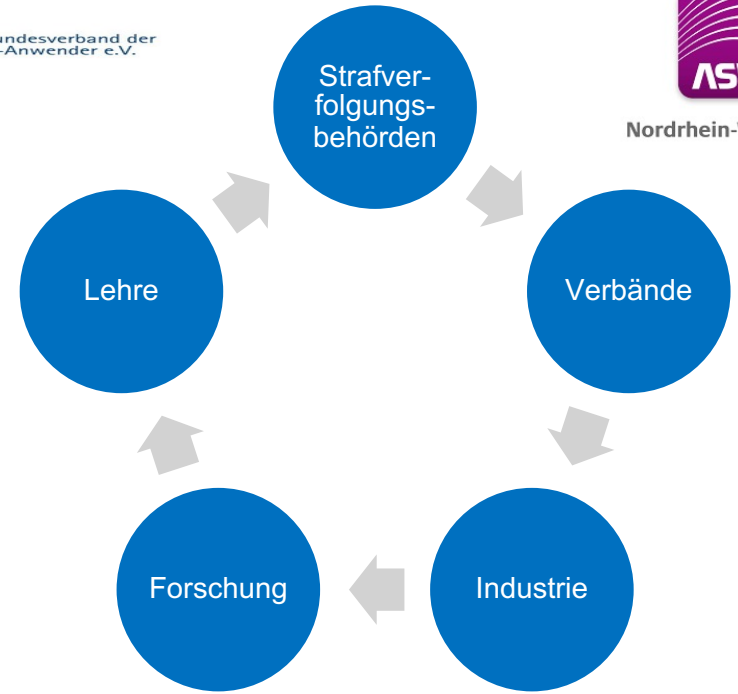
VOICE Bundesverband der IT-Anwender e.V.

bitkom

networker NRW
Der IT Verband

FH AACHEN
UNIVERSITY OF APPLIED SCIENCES

SMARTHOME
DEUTSCHLAND



ASW
Nordrhein-Westfalen

eco
Verband der
Internetwirtschaft e.V.

SWS
COMPUTERSYSTEME
Member of ACP Group

Fazit

POLIZEI
Nordrhein-Westfalen
Landeskriminalamt

- Cybercrime betrifft Behörden, Unternehmen und Privatleute gleichermaßen
- Die Fortschreitende Digitalisierung in allen Bereichen bietet neue Möglichkeiten für Straftäter
- Die Bekämpfung ist eine gesamtgesellschaftliche Aufgabe und es bedarf gemeinsamer Anstrengungen aller Akteure bei der Bekämpfung

Fragen?

Vielen Dank für Ihre Aufmerksamkeit.