DFN
DEUTSCHES FORSCHUNGSNETZ

POLIZEI
Nordrhein-Westfalen
Landeskriminalamt

bürgerorientiert · professionell · rechtsstaatlich

Cybercrime - eine unterschätzte Gefahr

whoami

Inna Claus LL.M

Kriminaloberkommissarin

Landeskriminalamt NRW

SG 41.1 – Cybercrime-Kompetenzzentrum

Tel.: 0211 939 4112

Fax: 0211 939 19 4112

inna.claus@polizei.nrw.de

Herausforderung Digitalisierung

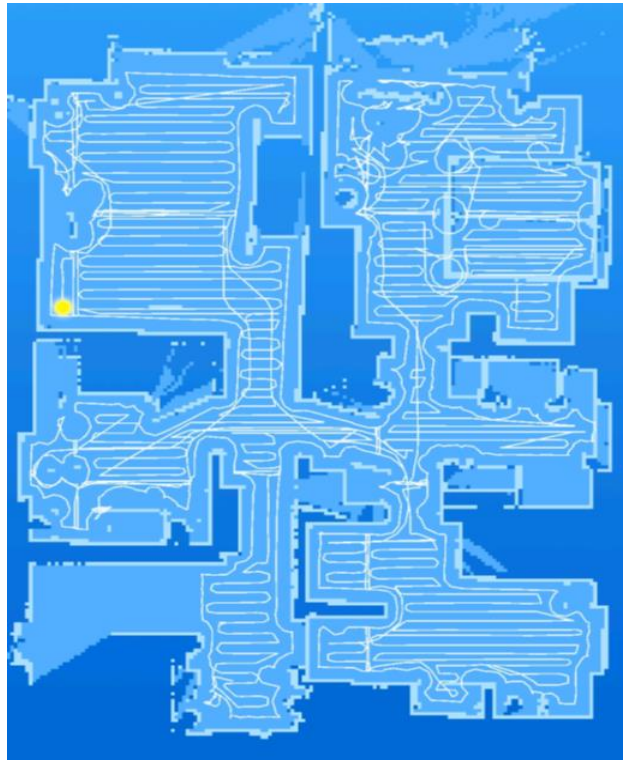

THE INTERNET IN 2023 EVERY MINUTE
60 SECONDS
22,831 visits to ChatGPT
241.2M emails sent
18.8M text messages sent
2.4M Google searches
694,000 video hours viewed
347,222 tweets
3.47M snaps created
10.4M viewing minutes
11,035 fake accounts removed
6.3M total Zoom meeting minutes
34,247 Slack messages
11,834 chats on Microsoft Teams
6.94M emoji sent
3.02M photos created with smartphones
271,309 IOS & Android app downloads
Created by: eDiscovery Today & LTMG

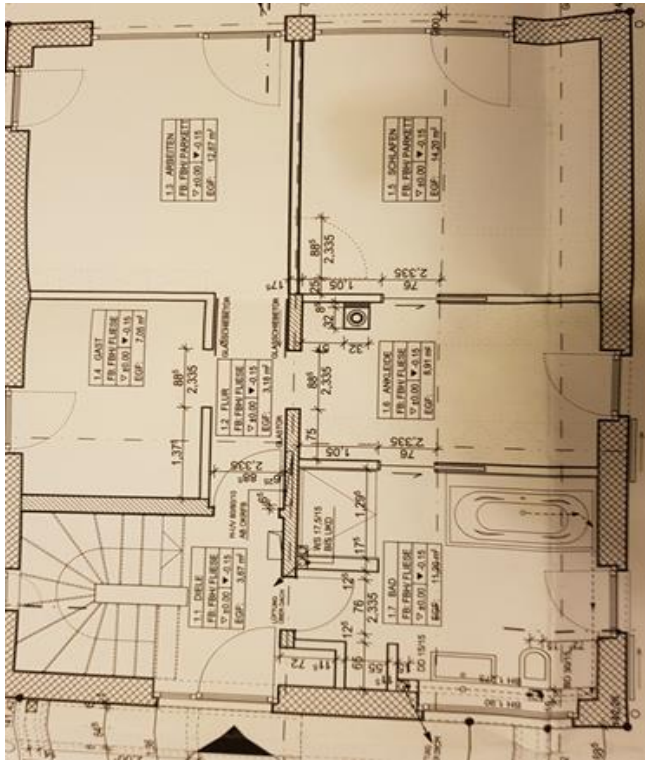
Digitales Umfeld

- Digitales Umfeld im Wandel
- Digitale Nutzer
- Neue Geschäftsmodelle und digitale Unternehmen
- Home Office
- E-Government

Digitales Umfeld

Digitales Umfeld





DFN

POLIZEI Nordrhein-Westfalen Landeskriminalamt

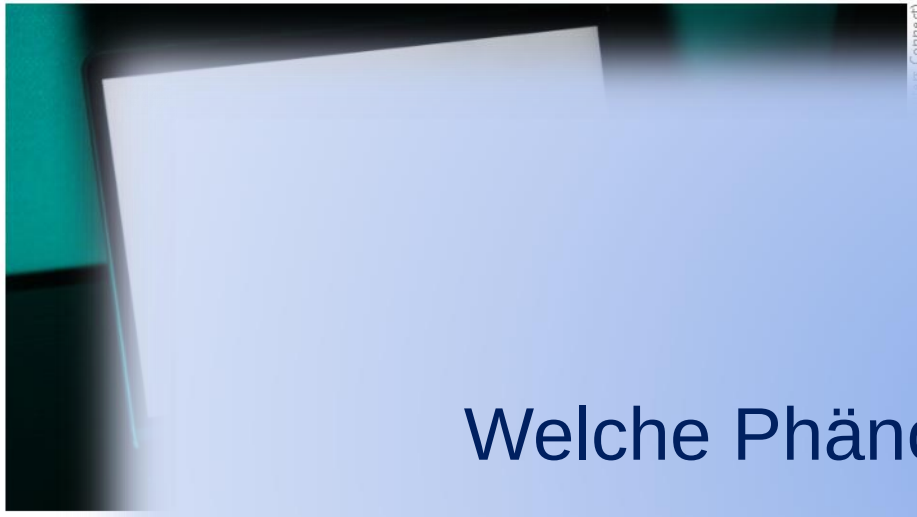
KI

CDU-Abgeordneter schiebt Nutzung von SA-Parole auf ChatGPT

KI-Angebote setzen sich zwar immer mehr durch, machen aber auch Fehler. Ein CDU-Politiker macht ChatGPT für eine Naziparole in einem Facebook-Post verantwortlich.

in Pocket speichern | merken

24. Februar 2024, 12:00 Uhr, Sebastian Grüner



KI

Deepfake eines Finanzchefs ermöglicht Millionenbetrug

Ein Angestellter überwies 23 Millionen Euro an Betrüger, die sich mithilfe von Deepfakes in einer Videokonferenz als seine Vorgesetzten ausgegeben haben.

in Pocket speichern | merken

4. Februar 2024, 12:34 Uhr, Andreas Donath

NACH CYBERANGRIFF

IT-Dienstleister kann Kundendaten nicht wiederherstellen

Ransomware-Hacker haben nicht nur Daten zahlreicher schwedischer Kunden von Tietoevry verschlüsselt, sondern ebenso die Back-ups und Logdateien des IT-Dienstleisters.

in Pocket speichern | merken

15. Februar 2024, 11:09 Uhr, Marc Stöckel

Welche Phänomene gibt es aktuell?

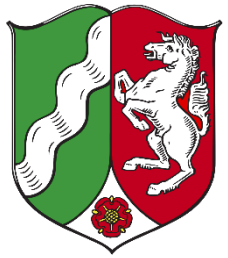
Trends und Phänomene Cybercrime

- Cyber-Erpressungen/ Ransomware
- (D)Dos-Angriffe
- Supply-Chain-Angriffe
- Phishing/ Spear-Phishing
- CEO-Fraud
- Identitätsdiebstahl
- KI-gestützten Phänomene
- Wirtschaftsspionage
- u.v.m

Wer sind die Täter? Wie sind sie motiviert?

- Monetär (bspw. Big Game Hunters)
- Politisch motiviert / HACKtivisten
- Staatlich gesteuert / instruiert (Spionage)
- Wirtschaftlich (Patenten, Datenbanken, Konkurrenzkampf)
- Selbstverherrlichung („Ich kann, was keiner kann“)
- Willkürlich zerstörerisch / Terroristisch

Was kostest „uns“ Cybercrime?



17.947.221 Einwohner

733 Mrd Euro BIP

Wirtschaftsstandort Nr. 1 in Deutschland

Wirtschaftsstandort Nr. 8 in Europa

730.600 KMU

Cybercrime als Gefahr für die Wirtschaft

88 % betroffene Unternehmen

630.960

- Anzahl der Unternehmen

223 Milliarden €

46,6 Milliarden €

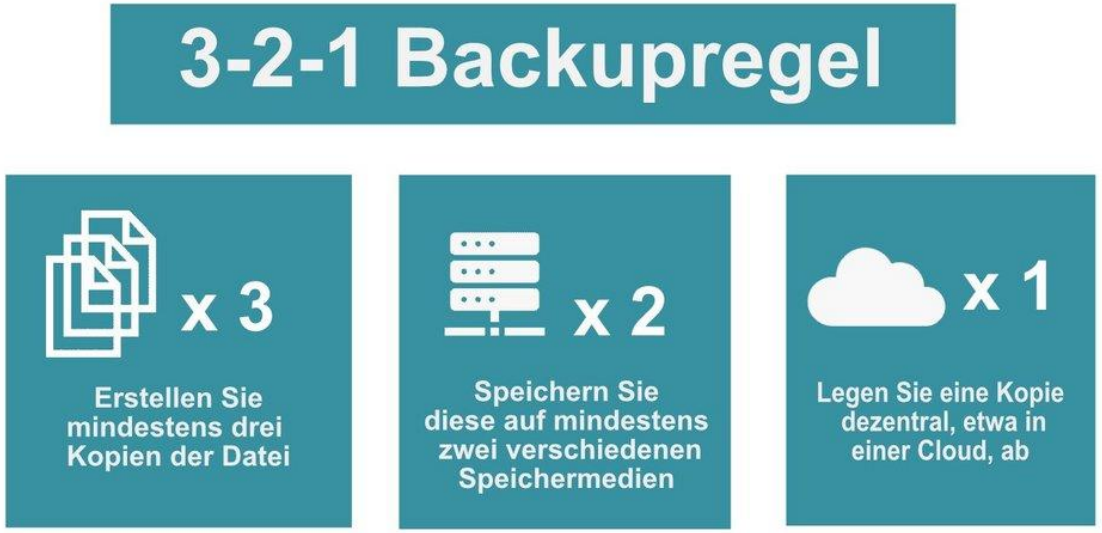
- Schäden im Jahr

Was kann man dagegen tun?


IN CASE OF
CYBERATTACK
BREAK GLASS
AND PULL CABLES

Wichtige Maßnahmen

- BackUp-Strategie (3-2-1 Regel)
- Patchmanagement
- Datenschutz und Datenintegrität, geeignete Übermittlungswege für sensible Informationen (Verschlüsselung, Passwort, 2-Faktor-Authentifizierung etc.)
- Firewall, Netzwerksegmentierung
- Administration, Dokumentation
- Physische Sicherheit der Infrastruktur
- Mitarbeitersensibilisierung, Fehlerkultur
- Notfallplan „Cybersicherheit“



Notfallmanagement

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

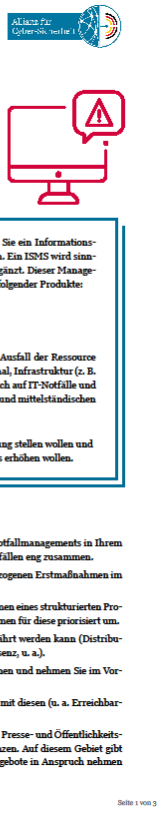
TOP 12 MASSNAHMEN BEI CYBER-ANGRIFFEN

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?



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.

Stand: September 2019 Seite 1 von 3

Was heißt das für die Polizei?

Single Point of Contact (24/7)

0211 939-4040

cybercrime.lka@polizei.nrw.de

Kooperationen
Gemeinsam gegen Cybercrime

bitkom

ASW
Nordrhein-Westfalen

eco
Verband der
Internetwirtschaft e.V.

networker NRW
Der IT Verband

FH AACHEN
UNIVERSITY OF APPLIED SCIENCES

Fraunhofer

Vielen Dank für die Aufmerksamkeit