



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



Bedrohungslage für Unternehmen (Bitkom, 2024)

- **81%** der Unternehmen betroffen, 10% unwissend
- **266,6 Milliarden Euro Schaden (Rekord)**
- 65% fühlen sich existenziell bedroht
- 70% der Angriffe durch organisierte Kriminalität, 20% durch Nachrichtendienste (Allokation nicht immer klar)
- Digitale Angriffe (74%) deutlich gestiegen
- Nur 53% der Unternehmen sind gut vorbereitet
- IT-Sicherheit macht mittlerweile ca. 17% des Gesamtbudgets aus

Herausforderung Digitalisierung

Digitales Umfeld

- Digitales Umfeld im Wandel
- Künstliche Intelligenz
- Neue Geschäftsmodelle und digitale Unternehmen
- Home Office
- E-Government, digitale Identität, digitale Geldbörse
- Smarthome



Wenn die Smartwatch weiß, dass du beim Trinken warst

<https://youtu.be/LefBfeKvIfw>

Computerpasswort wird mit einer Genauigkeit von 96% und eine PIN-Nummer, die an einem Geldautomaten eingegeben wurde, mit einer Genauigkeit von 87% wiederhergestellt

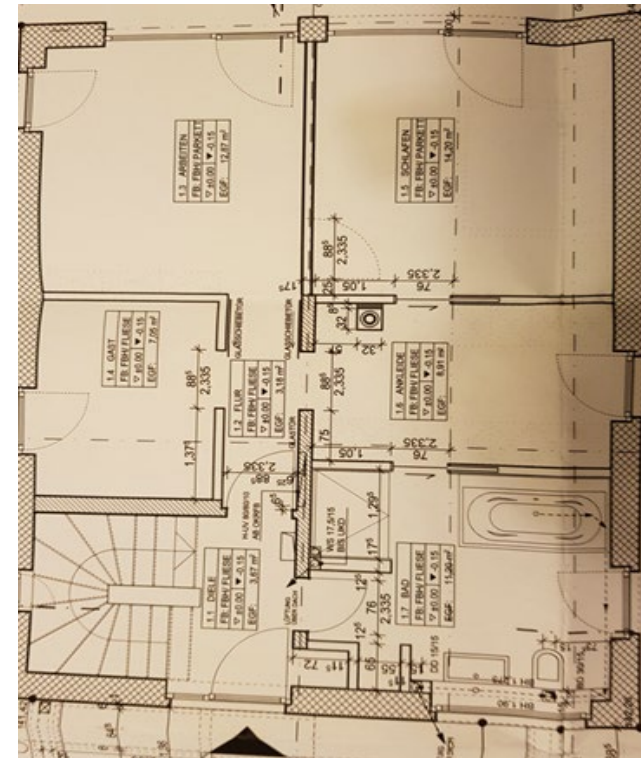


Quelle: Kaspersky
Lab

Digitales Umfeld



Digitales Umfeld



ADMIN-ZUGANG GEKAPERT

Insasse hackt Gefängnis-IT und macht Mithäftlinge reich

Aufgeflogen ist alles, weil Inhaftierte ihre Gier nicht im Griff hatten. Ein Millionenbetrag auf dem Konto eines Insassen ist dann doch etwas auffällig.

28. Oktober 2025 um 14:05 Uhr / Marc Stöckel

21

K1

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](#) [teilen](#)

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



DATENLECK BEI PORNOPLATTFORM

Hacker haben Nutzerdaten von Pornhub erbeutet

Eine bekannte Hackergruppe erpresst Pornhub mit Millionen von Datensätzen. Betroffen sind unter anderem Streaming-Aktivitäten von Premium-Nutzern.

16. Dezember 2025 um 08:52 Uhr / Marc Stöckel

4

News folgen



Bild: Ethion Miller/Getty

Welche Phänomene gibt es aktuell?

Trends und Phänomene Cybercrime

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

42 Fälle
2024



Ransomware Angriff auf die Südwestfalen IT

- Cyberangriff auf IT-Dienstleister für mehr als 70 Kommunen durch AKIRA
- Schwachstelle in der VPN Struktur wurde ausgenutzt
- Fehlende MFA die den Zugang zum Netzwerk erleichterte
- kompletter Ausfall der IT-Infrastruktur
- massive Auswirkungen

Ransomware-Angriff legt kommunalen IT-Dienstleister lahm

Südwestfalen-IT betroffen – Auswirkungen auf zahlreiche Kommunen



Im Juli 2023 erlebte Südwestfalen-IT (SIT), ein wichtiger IT-Dienstleister für mehr als 70 Kommunen in Nordrhein-Westfalen, einen schweren Ransomware-Angriff. Die Angreifer, die zur Gruppe „Akira“ gehören, nutzten eine Schwachstelle in der VPN-Infrastruktur der SIT, um unbefugten Zugang zu erhalten. Dieser Vorfall führte zu erheblichen Störungen in den IT-Systemen der betroffenen Kommunen und machte deutlich, wie verwundbar öffentliche IT-Dienstleister gegenüber Cyberbedrohungen sind.

Trends und Phänomene Cybercrime

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

231 Fälle
2024



14.02.2025, 17:30 Uhr

Audiobeitrag

🏠 > "Prorussische" Cyberattacke auf Staatsregierung und Polizei

"Prorussische" Cyberattacke auf Staatsregierung und Polizei

Nach BR-Informationen kam es vor Beginn der Sicherheitskonferenz zu einem stundenlangen Cyberangriff auf Webseiten von Staatsregierung und Polizei. Das Landesamt für Sicherheit in der Informationstechnik spricht von "prorussischem Hacktivismus".

NRW zählte 28 Cyber-Angriffe gegen Ministerien, Landesbetriebe und Behörden

Die Landesregierung in NRW zählte im vergangenen Jahr 28 Cyber-Angriffe auf Einrichtungen des Landes. Lediglich eine davon hatte größere Auswirkungen.

18.04.2023, 07:20 Uhr | Lesezeit: 2 Min. | Security

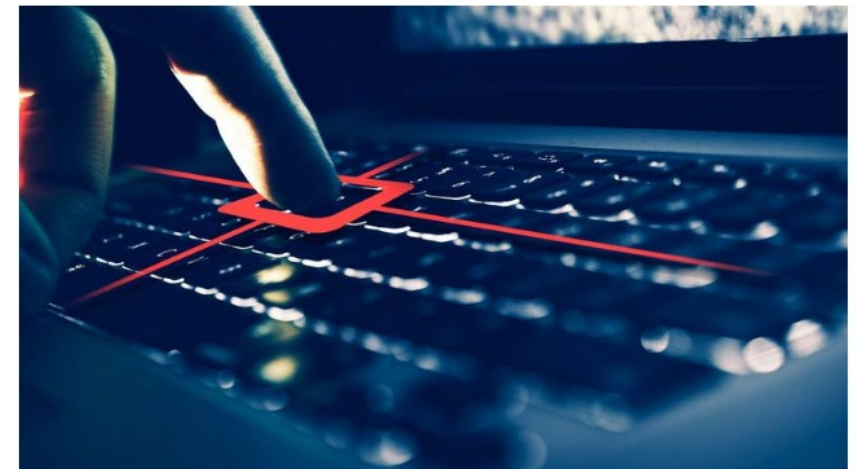


Cyberattacke auf Behörden

DDoS-Angriff legt über 30 Städte und Landkreise lahm

31.07.2025 · Von [Melanie Staudacher](#) · 3 min Lesedauer · 📌

Ein massiver DDoS-Angriff legte über 30 Kommunen in Sachsen-Anhalt und Thüringen lahm. Webseiten fielen stundenlang aus, eine ähnliche Attacke betraf Anfang Juli bereits die Arbeit von Rettungskräften. Dahinter werden pro-russische Hacker vermutet.



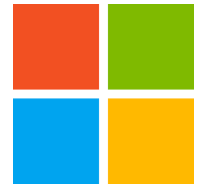
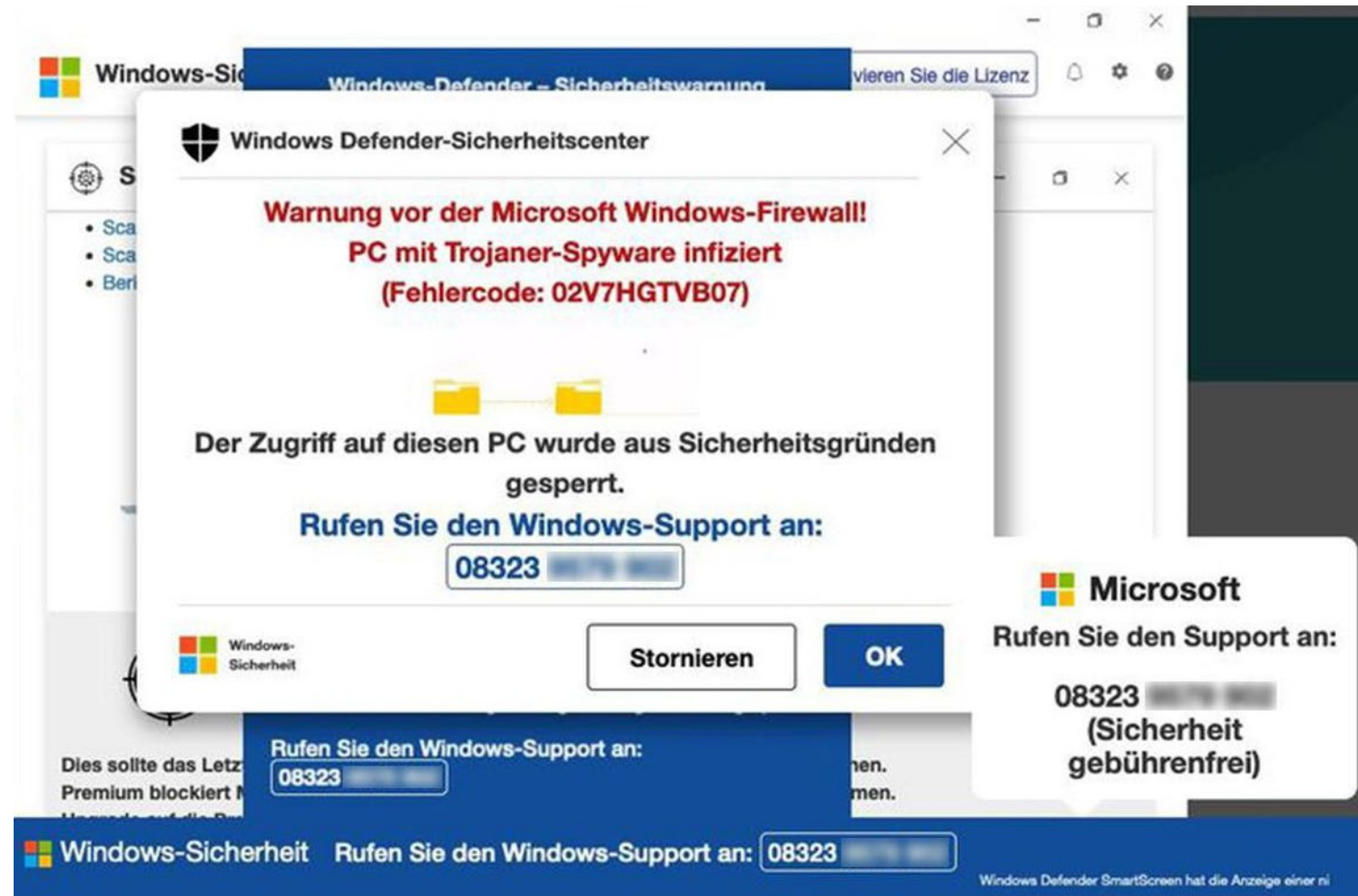
Ein DDoS-Angriff überflutet Server mit massenhaften Anfragen, bis sie überlasten und nicht mehr erreichbar sind. Die Folge: Webseiten, Dienste oder kritische Infrastruktur wie Notfallkommunikation können ausfallen.
(Bild: Tomasz Zaida - stock.adobe.com)

Trends und Phänomene Cybercrime

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







**506 Fälle
2024**

Trends und Phänomene Cybercrime

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

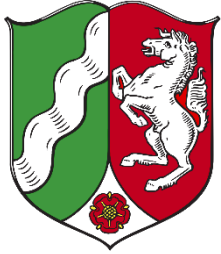


BEC Fraud – Gefälschte Rechnungen

- Stadt Dülmen hat im Februar 2024 rund **404.600€** für zwei neue Feuerwehrfahrzeuge überwiesen – leider an Betrüger
- Täuschung durch sehr realistisch gefälschte Rechnungen
- Täter verfügten über Insiderwissen und kannten den Beschaffungsprozess, hatten den Hersteller offenbar gezielt ausgespäht
- Trotz Vier-Augen-Prinzip und Prüfstelle wurde der Betrug nicht erkannt



Was kostest „uns“ Cybercrime?



18.01 Mio Einwohner

872 Mrd Euro BIP

Wirtschaftsstandort Nr. 1 in Deutschland

Wirtschaftsstandort Nr. 8 in Europa

717.160 KMU

Cybercrime als Gefahr für die Wirtschaft



**87 % betroffene
Unternehmen**



623.929

• Anzahl der Unternehmen



266 Milliarden €



56 Milliarden €

• Schäden im Jahr

Was kann man dagegen tun?



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“

3-2-1 Backupregel



Erstellen Sie
mindestens drei
Kopien der Datei



Speichern Sie
diese auf mindestens
zwei verschiedenen
Speichermedien



Legen Sie eine Kopie
dezentral, etwa in
einer Cloud, ab

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? | ✓ Wurden Maßnahmen unternommen, um das gesamte Maß der Ausbreitung festzustellen? Wurden alle angegriffenen Systeme identifiziert? |
| ✓ Haben Sie kontinuierlich Ihre Maßnahmen abgefragt, dokumentiert und an alle relevanten Personen und Verantwortlichen kommuniziert? | ✓ Wurden bei einem Cyber-Angriff geeigneten Schwachstellen in Systemen oder (Geschäfts-) Prozessen durch relevante Maßnahmen adressiert und behoben? |
| ✓ Wurden System-Protokolle, Log-Dateien, Notizen, Fotos von Bildschirmhalten, Datenträger und andere digitale Informationen forensisch gesichert? | ✓ Wurden, nach Abstimmung, die Polizei oder relevante Behörden (Datenschutz, Meldepflichten, etc.) benachrichtigt? |
| ✓ Haben Sie stets die besonders zeitkritischen und damit vorrangig zu schützenden Geschäftsprozesse im Fokus gehabt? | ✓ Wurden die Zugangsberechtigungen und Authentifizierungsmethoden für betroffene (geschäftliche und ggf. private) Accounts überprüft (z.B. neue Passwörter, 2FA)? |
| ✓ Wurden betroffene Systeme vom Netzwerk getrennt? Wurden Internetverbindungen zu den betroffenen Systemen getrennt? Wurden alle unautorisierten Zugriffe unterbunden? | ✓ Wird das Netzwerk nach dem Vorfall weiter überwacht, um mögliche erneute Anomalien festzustellen? |
| ✓ Wurden Backups getestet und vor möglichen weiteren Auswirkungen gesichert? | ✓ Wurden die betroffenen Daten und Systeme wiederhergestellt oder neu aufgebaut? |

Das Dokument ist ein gemeinsames Produkt wichtiger Organisationen: Bundesministerium, Chapter of Trust, Deutscher Industrie- und Handelskammertag e.V., ein - Verband der Internetwirtschaft e.V., Initiative Wirtschaftsschutz, Nationale Initiative für Informationssicherheit und Internet-Sicherheit e.V., NISIC - Bundesverband der IT-Anbieter e.V., Allianz für Cyber-Sicherheit des Bundesministeriums für Sicherheit in der Informationstechnik

Stand: September 2019

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 Notfallhandbuchs.

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 Personalarbeit. 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 Unterstützungsoptionen von Dienstleistern. Prüfen Sie vorab, ob Sie solche Angebote in Anspruch nehmen möchten und nehmen Sie frühzeitig Kontakt auf.

Stand: September 2019

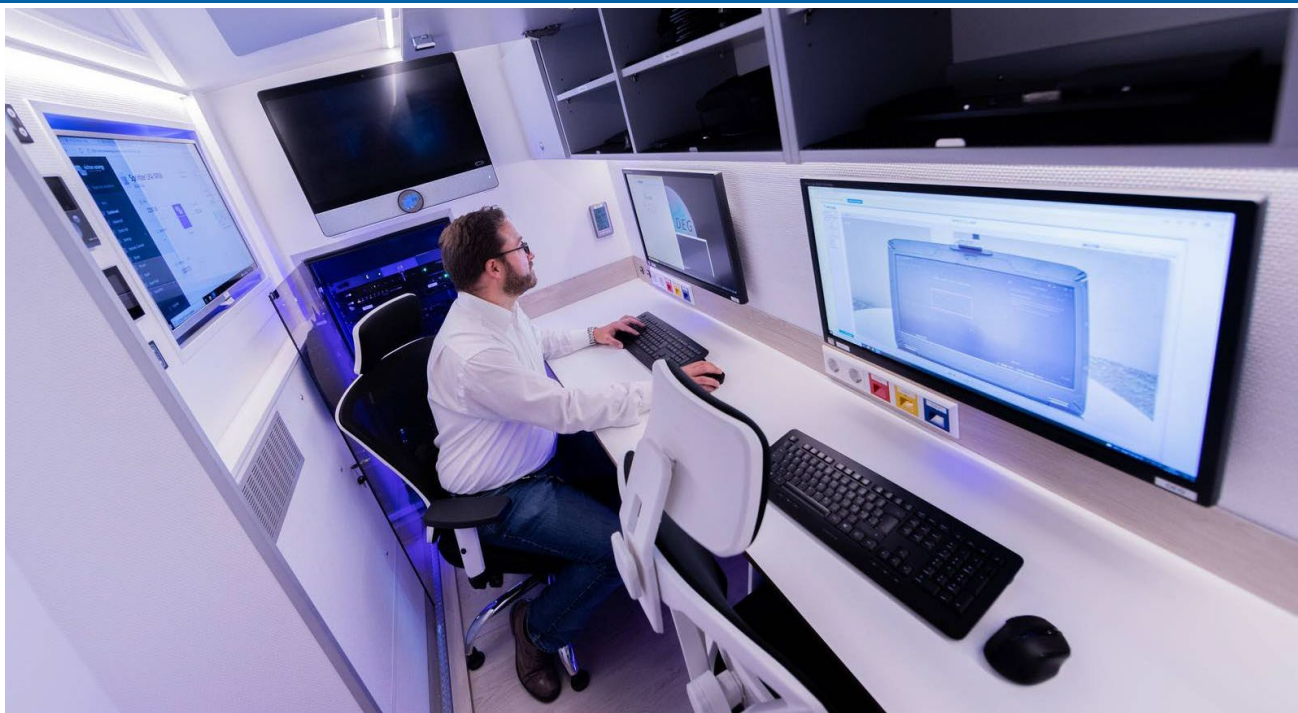
Seite 1 von 3

Was heißt das für die Polizei?

Single Point of Contact (24/7)

0211 939-4040
cybercrime.lka@polizei.nrw.de





Kooperationen Gemeinsam gegen Cybercrime



Vielen Dank für ihre Aufmerksamkeit!
Haben Sie noch Fragen?

Landeskriminalamt Nordrhein-Westfalen
Völklinger Str. 49, 40221 Düsseldorf
Telefon +49 211 939-4114
cybercrime.lka@polizei.nrw.de