POLIZEI
Nordrhein-Westfalen
Kreis Lippe

Arnd Begemann

Regierungsbeschäftigter (RBe)
- Kriminalprävention Cybercrime -

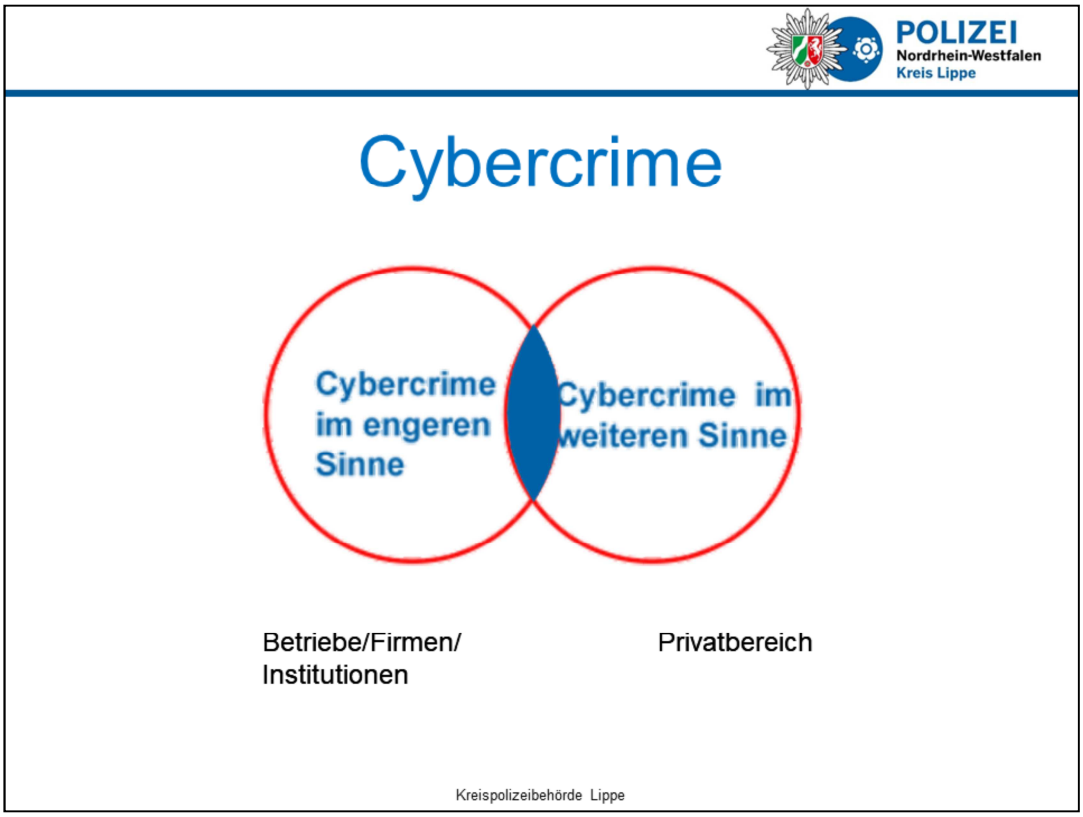
Kriminalkommissariat für
Kriminalprävention/Opferschutz (KK KP/O)
Friedrich-Petri-Str. 16
32791 Lage

rechtsstaatlich · bürgerorientiert · professionell

POLIZEI
Nordrhein-Westfalen
Kreis Lippe

Cybercrime ist Kriminalität unter Nutzung von Informations- und Kommunikationstechnik

Kreispolizeibehörde Lippe



Es gibt keine allgemein gültige Definition des Begriffs Computerkriminalität.

Gewöhnlich sind darunter alle Straftaten zusammengefasst, die unter Ausnutzung der digitalen Informations- und Kommunikationstechnik oder gegen diese begangen werden.

Im polizeilichen Bereich wird darüber hinaus zwischen Computerkriminalität *im engeren Sinn* und Computerkriminalität *im weiteren Sinn* unterschieden.

Cybercrime im engeren Sinne (meistens Firmen u. Institutionen)

umfasst jene Straftaten, bei denen Angriffe auf Daten oder Computersysteme unter Ausnutzung der Informations- und Kommunikationstechnik begangen werden.

(zum Beispiel Datenbeschädigung, Hacking, DDoS-Attacken).

Unter **Cybercrime im weiteren Sinne(Privatbereich)**

versteht man Straftaten, bei denen die Informations- und Kommunikationstechnik **zur Planung, Vorbereitung und Ausführung für herkömmliche Kriminaldelikte** eingesetzt wird.

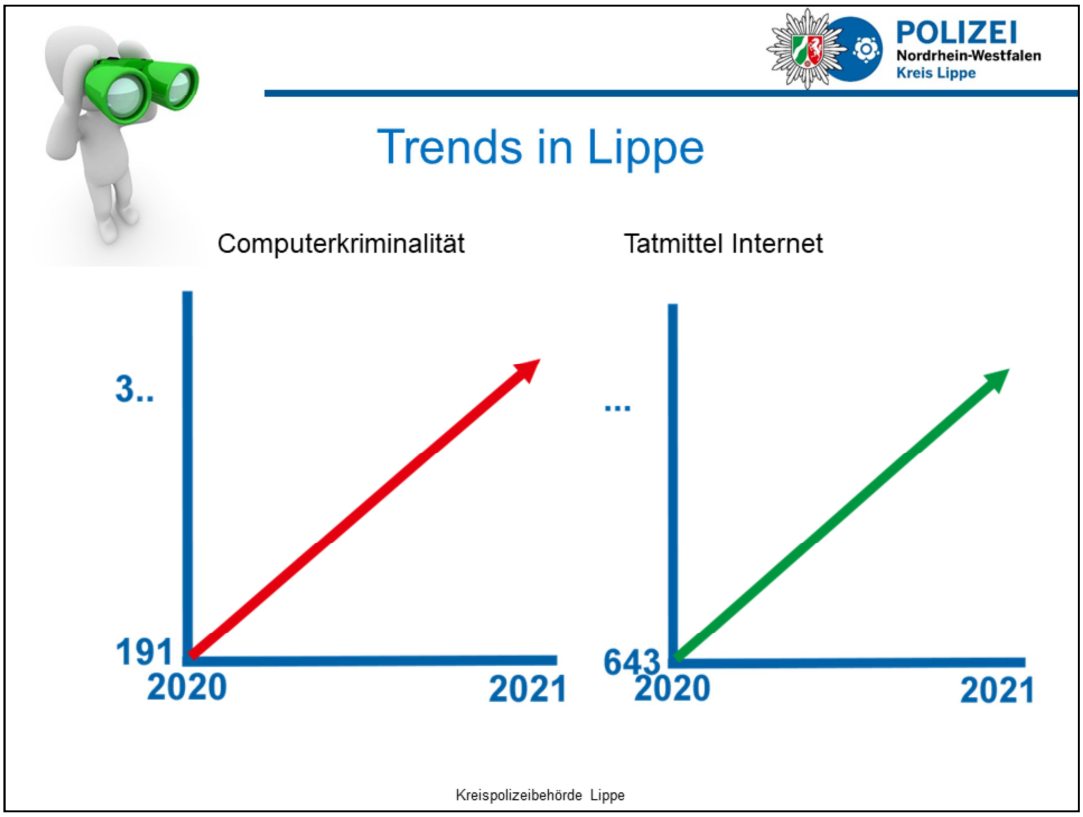
Beispiele: Betrugsdelikte, Kinderpornografie, Cyber-Grooming (Anbahnung) oder Cyber-Mobbing.

Diese Straftaten können praktisch jede Form von Kriminalität annehmen.

Für **Cybermobbing** gibt es keine eigenen Gesetzesvorlage deshalb fallen:

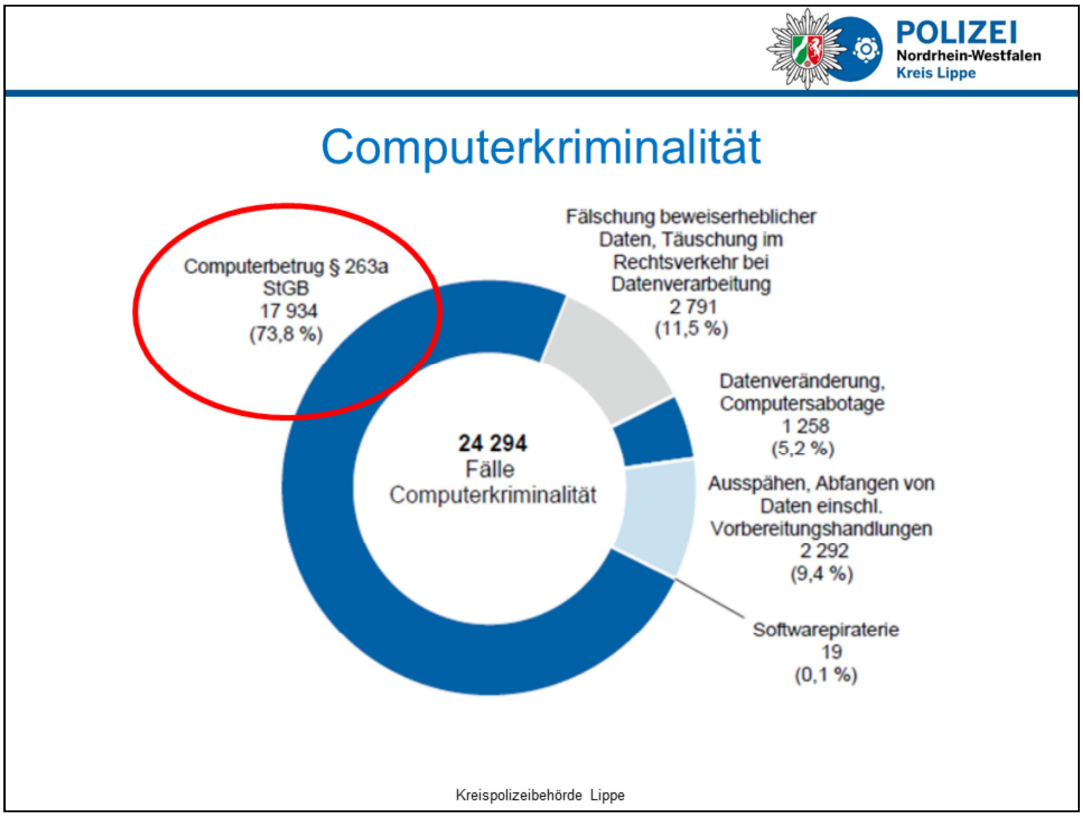
- Stalkings § 238 StGB
- Beleidigung § 185 StGB
- Verleumdung (ist eine Beleidigung) § 187 StGB
- Üble Nachrede (ist eine Beleidigung) § 186 StGB
- Nötigung § 240 StGB
- Erpressung § 253 StGB
- Verletzung des höchstpersönlichen Lebensbereichs durch Bildaufnahmen § 201 a
- Recht am eignen Bild § 22 KUG (Gesetz betreffend das Urheberrecht an Werken der bildenden Künste und der Photographie)
- Verletzung der Vertraulichkeit des Wortes § 201 StGB
- …

darunter.



Wir bewegen uns hier im Hellfeld!

Was ist mit dem Dunkelfeld? (Viel höhere Zahlen)



§ 263a Computerbetrug Strafgesetzbuch (StGB)

Computerprogramme Zwecke des Betrugs benutzt, bzw. der Beeinflussung von Daten benutzt

*Vermögen des anderen beschädigt

*Beeinflussung von Daten durch Schadecode

*Unbefugte Verwendung/unbefugte Einwirkung ->Freiheitsstrafe bis zu 5 Jahren oder Geldstrafe

(1)Wer Computerprogramme herstellt, sich oder einem anderen verschafft, feilhält, verwahrt oder einem anderen überlässt ->Freiheitsstrafe bis zu 3 Jahren oder Geldstrafe

(2)Passwörter oder sonstige Sicherungscodes, die zur Begehung einer solchen Tat geeignet sind, herstellt, sich oder einem anderen verschafft, feilhält, verwahrt oder einem anderen überlässt

->Freiheitsstrafe bis zu 5 Jahren oder Geldstrafe

§ 269 Fälschung beweiserheblicher Daten

(1) Wer zur Täuschung im Rechtsverkehr beweiserhebliche Daten so speichert oder verändert, dass bei ihrer Wahrnehmung eine unechte oder verfälschte Urkunde vorliegen würde, oder derart gespeicherte

oder veränderte Daten gebraucht, wird mit Freiheitsstrafe bis zu fünf Jahren oder mit Geldstrafe bestraft.

*Manipulation des Guthabens auf einer Guthabenkarte
*nachgemachte E-Mails, die zum Beispiel den Anschein erwecken, von einer Bank zu stammen (Phishing)
*nachgemachte Websites, die ebenfalls den Anschein vermitteln sollen, sie würden von einer Bank oder einem anderen Anbieter stammen.
*Auftreten unter fremdem Namen (Identitätsdiebstahl)

§ 270 Täuschung im Rechtsverkehr bei Datenverarbeitung

Der Täuschung im Rechtsverkehr steht die fälschliche Beeinflussung einer Datenverarbeitung im Rechtsverkehr gleich.

Täuschung ist durch fälschliche Beeinflussung einer Datenverarbeitung im Rechtsverkehr zu ersetzen!

*Manipulation des Guthabens auf einer Guthabenkarte

*nachgemachte E-Mails, die zum **Beispiel** den Anschein erwecken, von einer Bank zu stammen (Phishing)

§ 303a Datenveränderung (Virtuelle Sachbeschädigung)

(1) Wer rechtswidrig Daten (§ 202a Abs. 2) löscht, unterdrückt, unbrauchbar macht oder verändert, wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft.

(2) Der Versuch ist strafbar.

(3) Für die Vorbereitung einer Straftat nach Absatz 1 gilt § 202c entsprechend.

Verteilen von Computerviren, die Daten überschreiben und/oder löschen. Dadurch wir der Datenbestand des Computers verändert.

Einschleusen, installieren, mailen von Computerviren, die das Computersystem beeinträchtigen

§ 303b Computersabotage

(1) Wer eine Datenverarbeitung, die für einen anderen von wesentlicher Bedeutung ist, dadurch erheblich stört, dass er1.eine Tat nach § 303a Abs. 1 begeht,

2.Daten (§ 202a Abs. 2) in der Absicht, einem anderen Nachteil zuzufügen, eingibt oder übermittelt oder

3.eine Datenverarbeitungsanlage oder einen Datenträger **zerstört, beschädigt, unbrauchbar macht, beseitigt oder verändert,**

wird mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft.

(2) Handelt es sich um eine Datenverarbeitung, die für einen fremden Betrieb, ein **fremdes Unternehmen oder eine Behörde von wesentlicher Bedeutung ist**, ist die Strafe Freiheitsstrafe **bis zu fünf Jahren oder** Geldstrafe.(KRITIS)

(3) Der Versuch ist strafbar.

(4) In besonders schweren Fällen des Absatzes 2 ist die Strafe Freiheitsstrafe von **sechs Monaten bis zu zehn Jahren.** Ein besonders schwerer Fall liegt in der Regel vor, wenn der Täter

1.einen **Vermögensverlust großen Ausmaßes herbeiführt,**

2.gewerbsmäßig oder als Mitglied einer Bande handelt, die sich zur fortgesetzten Begehung von Computersabotage verbunden hat,

3.durch die Tat die **Versorgung der Bevölkerung mit lebenswichtigen Gütern oder Dienstleistungen oder die Sicherheit der Bundesrepubli**k Deutschland beeinträchtigt.

(5) Für die Vorbereitung einer Straftat nach Absatz 1 gilt § 202c entsprechend.

§ 202a Ausspähen von Daten

(1) Wer unbefugt sich oder einem anderen Zugang zu Daten, **die nicht für ihn bestimmt** und die gegen unberechtigten Zugang besonders gesichert sind, unter Überwindung der Zugangssicherung verschafft,

wird mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft.

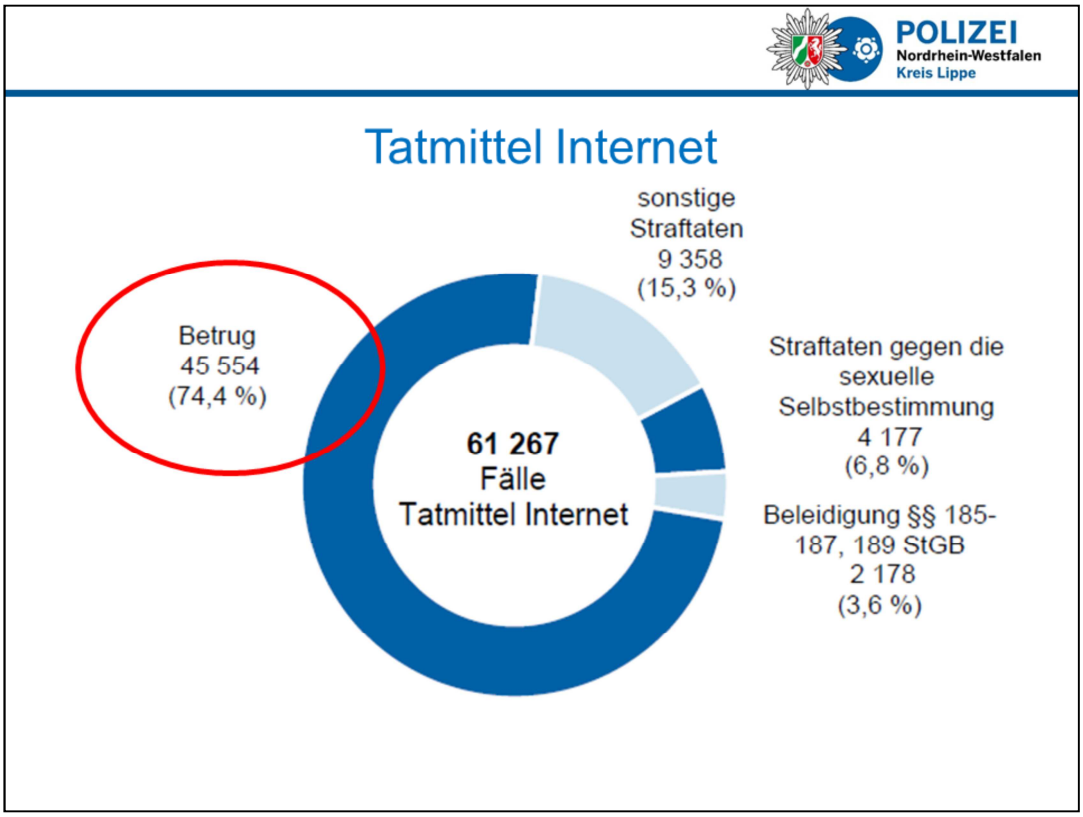
(2) Daten im Sinne des Absatzes 1 sind nur solche, die elektronisch, magnetisch oder sonst nicht unmittelbar wahrnehmbar gespeichert sind oder übermittelt werden.

§ 202b Abfangen von Daten

Wer unbefugt sich oder einem anderen unter Anwendung von technischen Mitteln nicht für ihn bestimmte Daten (§ 202a Abs. 2) aus einer nichtöffentlichen Datenübermittlung oder aus der elektromagnetischen Abstrahlung einer Datenverarbeitungsanlage verschafft, wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft, wenn die Tat nicht in anderen Vorschriften mit schwererer Strafe bedroht ist.

Softwarepiraterie keine Einzelnormen

§106 UrhG, §17 UWG,§ 202a StGB, $2 II UrhG



§ 263 Betrug StGB

(1) Wer in der Absicht, sich oder einem Dritten einen rechtswidrigen Vermögensvorteil zu verschaffen, das Vermögen eines anderen dadurch beschädigt, dass er durch Vorspiegelung falscher oder durch Entstellung oder Unterdrückung wahrer Tatsachen einen Irrtum erregt oder unterhält, wird mit Freiheitsstrafe bis zu fünf Jahren oder mit Geldstrafe bestraft.

(2) Der Versuch ist strafbar.

(3) In besonders schweren Fällen ist die Strafe Freiheitsstrafe von sechs Monaten bis zu zehn Jahren. Ein besonders schwerer Fall liegt in der Regel vor, wenn der Täter1.gewerbsmäßig oder als Mitglied einer Bande handelt, die sich zur fortgesetzten Begehung von Urkundenfälschung oder Betrug verbunden hat,

2.einen Vermögensverlust großen Ausmaßes herbeiführt oder in der Absicht handelt, durch die fortgesetzte Begehung von Betrug eine große Zahl von Menschen in die Gefahr des Verlustes von Vermögenswerten zu bringen,

3.eine andere Person in wirtschaftliche Not bringt,

4.seine Befugnisse oder seine Stellung als Amtsträger oder Europäischer Amtsträger missbraucht oder

5.einen Versicherungsfall vortäuscht, nachdem er oder ein anderer zu

diesem Zweck eine Sache von bedeutendem Wert in Brand gesetzt oder durch eine Brandlegung ganz oder teilweise zerstört oder ein Schiff zum Sinken oder Stranden gebracht hat.

(4) § 243 Abs. 2 sowie die §§ 247 und 248a gelten entsprechend.

(5) Mit Freiheitsstrafe von einem Jahr bis zu zehn Jahren, in minder schweren Fällen mit Freiheitsstrafe von sechs Monaten bis zu fünf Jahren wird bestraft, wer den Betrug als Mitglied einer Bande, die sich zur fortgesetzten Begehung von Straftaten nach den §§ 263 bis 264 oder 267 bis 269 verbunden hat, gewerbsmäßig begeht.

(6) Das Gericht kann Führungsaufsicht anordnen (§ 68 Abs. 1).

(7) (weggefallen)

§ 185 Beleidigung

Die Beleidigung wird mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe und, wenn die Beleidigung öffentlich, in einer Versammlung, durch Verbreiten eines Inhalts (§ 11 Absatz 3) oder mittels einer Tätlichkeit begangen wird, mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft.

§ 186 Üble Nachrede

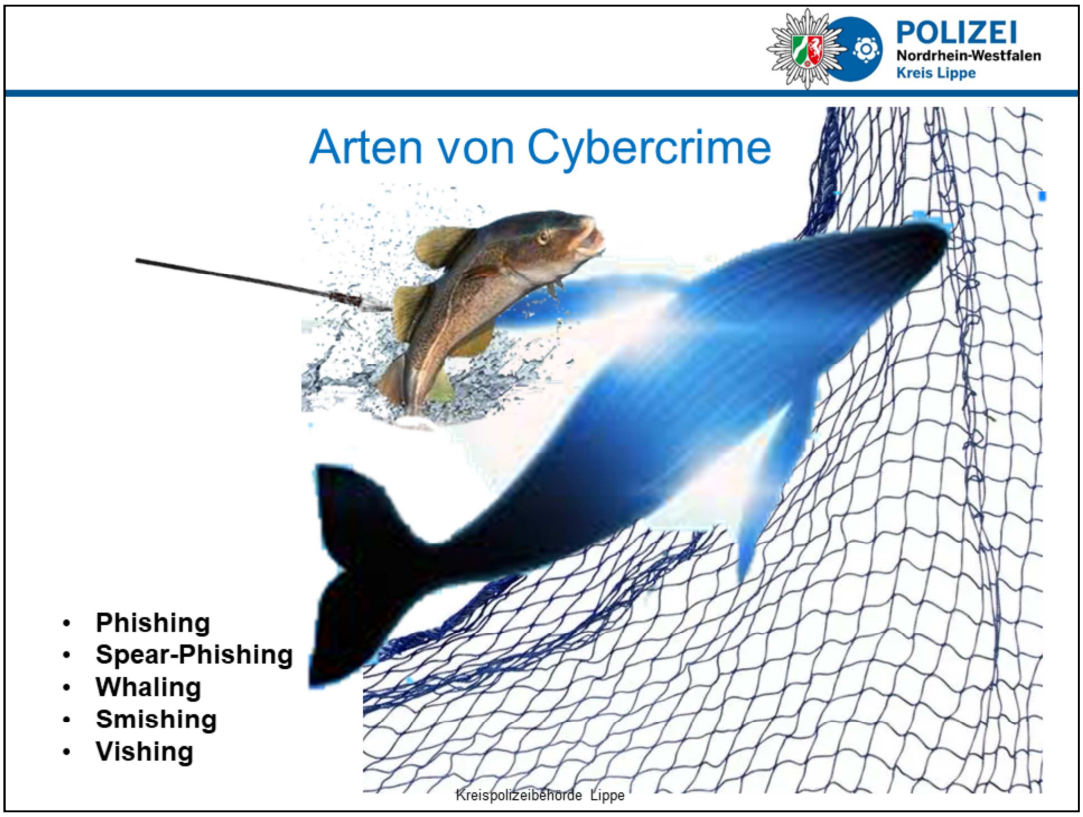
Wer in Beziehung auf einen anderen eine Tatsache behauptet oder verbreitet, welche denselben verächtlich zu machen oder in der öffentlichen Meinung herabzuwürdigen geeignet ist, wird, wenn nicht diese Tatsache erweislich wahr ist, mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe und, wenn die Tat öffentlich, in einer Versammlung oder durch Verbreiten eines Inhalts (§ 11 Absatz 3) begangen ist, mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft.

§ 187 Verleumdung

Wer wider besseres Wissen in Beziehung auf einen anderen eine unwahre Tatsache behauptet oder verbreitet, welche denselben verächtlich zu machen oder in der öffentlichen Meinung herabzuwürdigen oder dessen Kredit zu gefährden geeignet ist, wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe und, wenn die Tat öffentlich, in einer Versammlung oder durch Verbreiten eines Inhalts (§ 11 Absatz 3) begangen ist, mit Freiheitsstrafe bis zu fünf Jahren oder mit Geldstrafe bestraft.

§ 189 Verunglimpfung des Andenkens Verstorbener

Wer das Andenken eines Verstorbenen verunglimpft, wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft.



Phishing kein gezieltes Ausspähen von Daten, versenden vom Massen-E-Mails bzw. versenden von Daten mit einem Link (Netz auswerfen).

Empfänger verleitet werden, persönliche, finanzielle oder sicherheitsbezogene Informationen preiszugeben.

Aktuell im Zusammenhang mit der Ukraine-Krise wird versucht sich als Ban auszugeben und es neue Sanktionen der Banken geben würde und deshalb muss man sich neu verifizieren.

Spear-Phishing direktes Ausspähen z.B. auf den Chef (gezielt den Speer benutzen).

Whaling od. Whalephishing ist auch als CEO-Betrug bekannt. ... Es ähnelt dem **Phishing** insofern, dass Zielpersonen durch Methoden wie E-Mail und Webseiten-Spoofing dazu verleitet werden sollen, bestimmte Aktionen durchzuführen, beispielsweise das Offenlegen vertraulicher Daten oder das Übertragen von Geld.

Vishing Unerbetene Anrufe um Daten rauszugeben.

E-Mailspoofing Veränderung des Mailheaders mit falschen Absenderadressen

IP-Spoofing Der Header eines Datenpaketes wird mit falschen Absenderinformationen gesende.t

Phishing-Angriff: Unter einem Phishing-Angriff versteht man Versuche,

sich über gefälschte **Webseiten, E-Mails und Kurznachrichten** als vertrauenswürdiger Kommunikationspartner in einer elektronischen Kommunikation auszugeben.

Whaling-Phishing-Angriff: Es ist häufiger Cyberangriff, bei dem ein Angreifer Spear-Phishing-Methoden einsetzt, um ein großes, hochrangiges Ziel, wie z. B. die Führungsetage, anzugreifen.

Social Engineering Beim Social Engineering nutzt der Täter den "Faktor Mensch" als vermeintlich schwächstes Glied der Sicherheitskette aus, um seine kriminelle Absicht zu verwirklichen.

Anrufe, Mails, etc. vertrauen schaffen !!! Aufstöbern von verschiedenen Daten aus verschiedenen Kanälen.

Vorbereitung oft über Social Engineering

Social Engineering [ˈsəʊʃl ˌɛndʒɪˈnɪəɹɪŋ] (engl. eigentlich „angewandte Sozialwissenschaft“, auch „soziale Manipulation“) nennt man **zwischenmenschliche Beeinflussungen** mit dem Ziel, bei Personen bestimmte Verhaltensweisen hervorzurufen, sie zum Beispiel zur Preisgabe von vertraulichen Informationen, zum Kauf eines Produktes oder zur Freigabe von Finanzmitteln zu bewegen.

POLIZEI
Nordrhein-Westfalen
Kreis Lippe

Tipps

- geben sie keine pers. Informationen des Chefs am Telefon od. Mail weiter

Sensibilisierung der Mitarbeiter

- allg. Sensibilisierung der Kolleg:innen zu diesem Themen
- schauen Sie sich die Mails zuerst in der Vorschau an
- fragen Sie einen Kolleg:innen ob er/sie einmal mit über die besagte Mail schaut. (Vier-Augen-Prinzip)
- schauen sie sich den Kopf der Mail genau an. Lassen Sie sich die genaue Absenderadresse anzeigen. (Gmail-Adressen, o.ä. im Zusammenhang mit Zahlungsanweisungen sind sehr verdächtig)
- Zahlenkombinationen in der Mailadresse sind sehr verdächtig
- öffnen Sie keine Links in der Mail/SMS
- drücken Sie auf keinen Button(Knopf) in der Mail

POLIZEI
Nordrhein-Westfalen
Kreis Lippe

Tipps

- rufen Sie die jeweilige bzw. Ihre Bank an ob es weitere Vorfälle dieser Art schon bekannt sind
- rufen Sie den Absender an, wenn er sich mit einer Firmenadresse ausgibt und klären Sie die Situation ab
- leiten Sie diese Mail nicht weiter, ihre Firma(die Domain der Firma/Institution) könnte auf eine Black List kommen
- legen Sie die Mail in einem separaten Ordner ab (Beweissicherung), wenn Sie rechtliche Schritte einleiten möchten
- machen Sie Screenshots von der Mail und dem Inhalt(Beweissicherung) wenn nötig
- fragen Sie ihren Medienbeauftragten, Datenschutzbeauftragten und/oder einen Systemadministrator über weitere Vorgehensweisen
- sperren Sie die Absenderadresse im Spamfilter (den Administrator fragen)

POLIZEI
Nordrhein-Westfalen
Kreis Lippe

Phishingmails aktuell

Sparkasse

Sehr geehrt [redacted]

Um den Schutz für Ihr Sparkassenkonto zu erhöhen, haben wir das neue Sparkassen Fingerprint System (SFS) entwickelt.

Das Sparkassen Fingerprint System (SFS) ist ein auf künstlicher Intelligenz basierendes Sicherheitssystem und ist daher einmalig in der EU & bietet ihnen die maximal mögliche Sicherheit im Online-Banking.

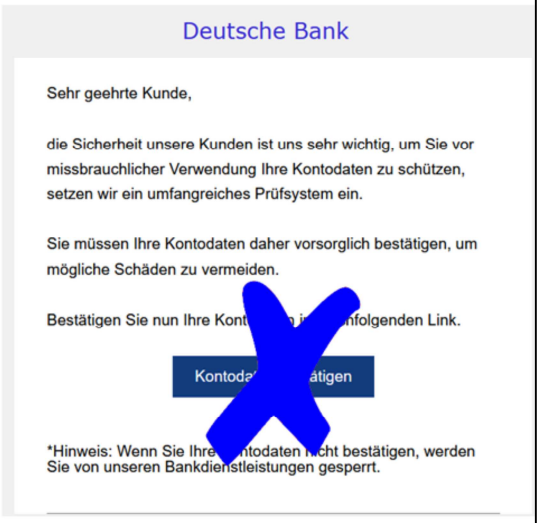
Die künstliche Intelligenz erstellt für jeden Kunden ein eigenes Profil und kann dadurch mit enormer Präzession bestimmen, ob es sich um ein legitimen Login Versuch handelt. Hierdurch wird jeder unautorisierter Login Versuch direkt blockiert.

Damit künstliche Intelligenz dieses Profil auch für ihr Konto erstellen kann, ist eine Umstellung mit abschließender Verifizierung ihres Kontos notwendig. Bitte führen Sie die Kontoerstellung bis zum 04.04.2022 durch. [illegible] Konten, die bis zum Stichtag nicht auf das neue System umgestellt wurden, werden vo[illegible]eaktiviert.

Für die Kontoerstellung wird sich ein Berater[illegible]er Dateneingabe mit Ihnen in Verbindung setzen.

[illegible]

Mit freundlichen Grüßen
Ihr Service Team



Deutsche Bank

Sehr geehrte Kunde,

die Sicherheit unsere Kunden ist uns sehr wichtig, um Sie vor missbrauchlicher Verwendung Ihre Kontodaten zu schützen, setzen wir ein umfangreiches Prüfsystem ein.

Sie müssen Ihre Kontodaten daher vorsorglich bestätigen, um mögliche Schäden zu vermeiden.

Bestätigen Sie nun Ihre Kont[illegible]nfolgenden Link.

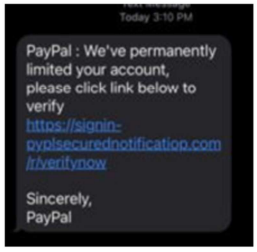
Kontoda[illegible]ätigen

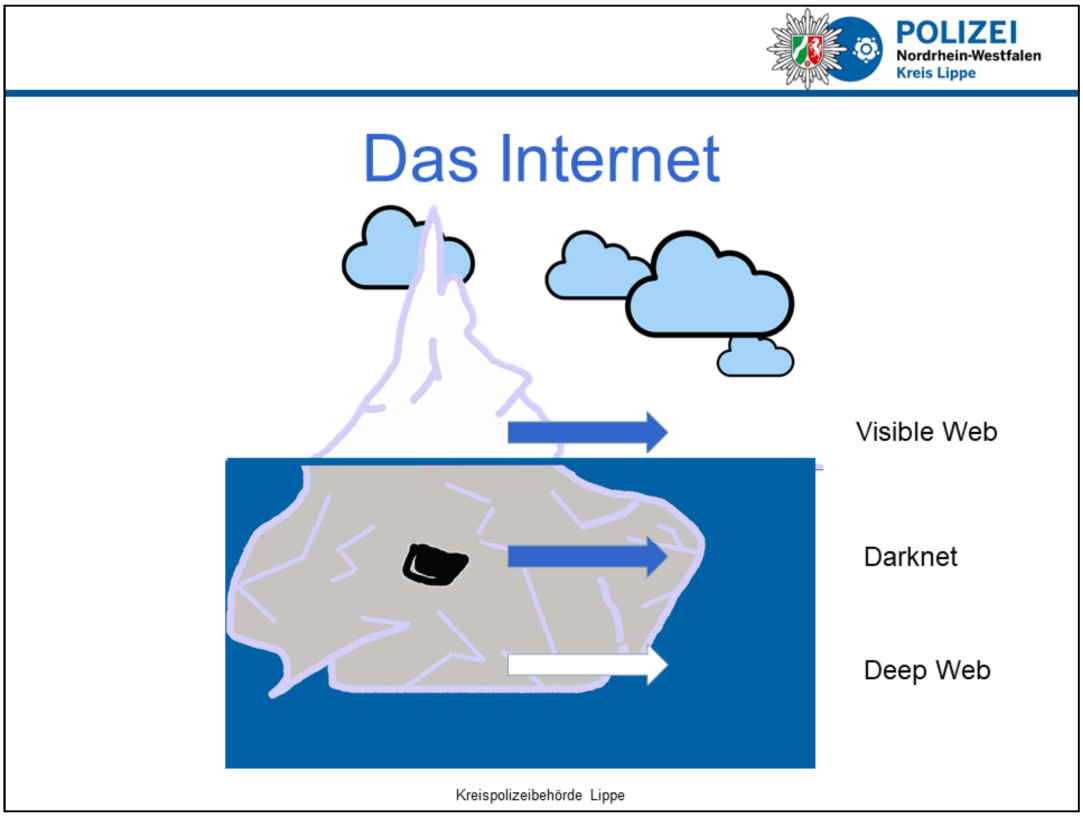
*Hinweis: Wenn Sie Ihre[illegible]ntodaten nicht bestätigen, werden Sie von unseren Bankdienstleistungen gesperrt.

Kreispolizeibehörde Lippe

POLIZEI
Nordrhein-Westfalen
Kreis Lippe

Smishing aktuell





Surface Web, Visible Web oder Clear Net = finden über Google etc.

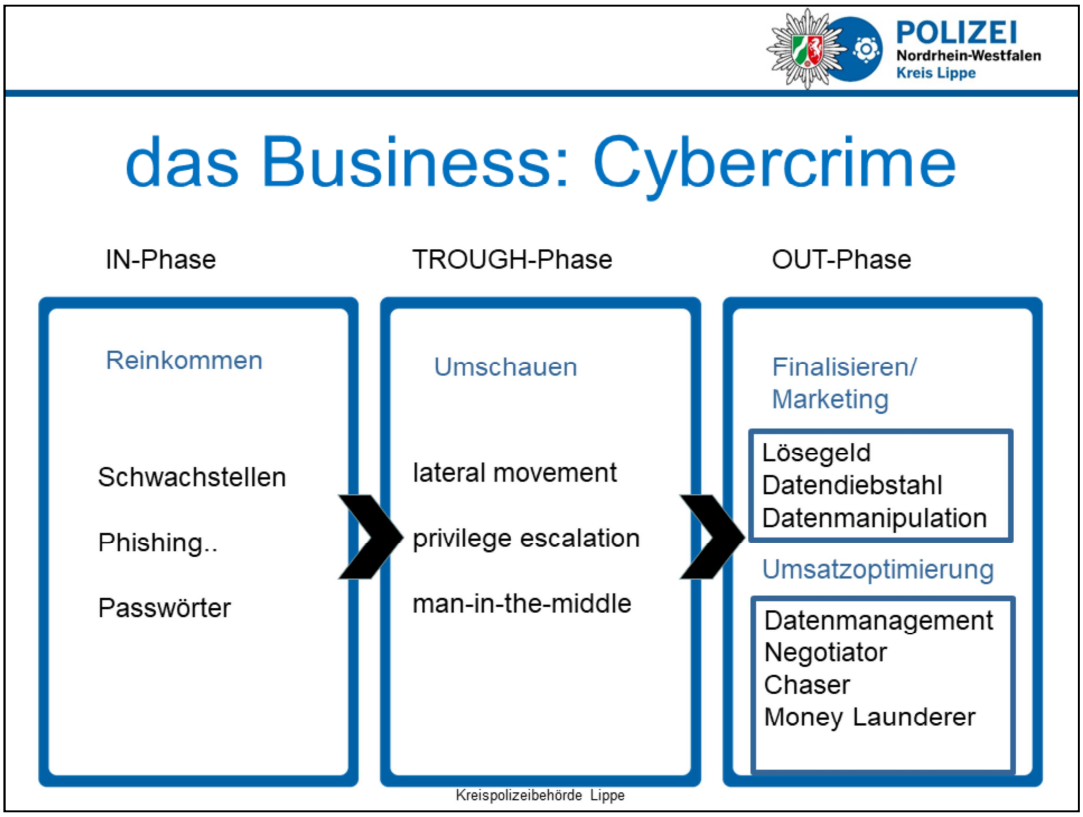
Surface = Oberfläche

Deep Web bis zu 500 x größer als das von Suchmaschinen wie Google genutzte oder Visible Net

für Suchmaschinen sichtbare Surface Web oder Visible Net

Das Darknet hingegen ein kleiner Teil des Deep Web und ist durch den Torbrowser im (Onion-Netzwerk) erreichbar.

Hier tummeln sich „dubiose Gestalten“! Adressen werden gehandelt und … !



Buisiness:

1. **Zufällige Opfer durch Massenangriffe**
2. **Gezielte Opfer durch Aufträge aus dem Internet bzw. Darknet angreifen**

Schwachstellen wie Portscannen

Phishing…

Passwörter: Brute Force Angriffe

(1)IN-Phase in das System kommen

Schwachstellen, Phishing, Vishing, Passwörter, Social Engineering,

(2) Troughphase Umschauen, abwarten Tee trinken ☺

lateral movement: im Netzwerk bewegen und das Angriffsziel sondieren

privilege escalation: Als Rechteausweitung, auch Rechteerhöhung, Privilegien Erweiterung oder Privilegien-Eskalation genannt, bezeichnet man **die Ausnutzung eines Computerbugs bzw. eines Konstruktions- oder Konfigurationsfehlers** einer Software mit dem Ziel, einem Benutzer oder einer Anwendung Zugang zu Ressourcen zu verschaffen, deren

Nutzung mit eingeschränkten Rechten nicht möglich ist.

Mitlesen von E-Mails: Man-in-the-Middle Angriffe

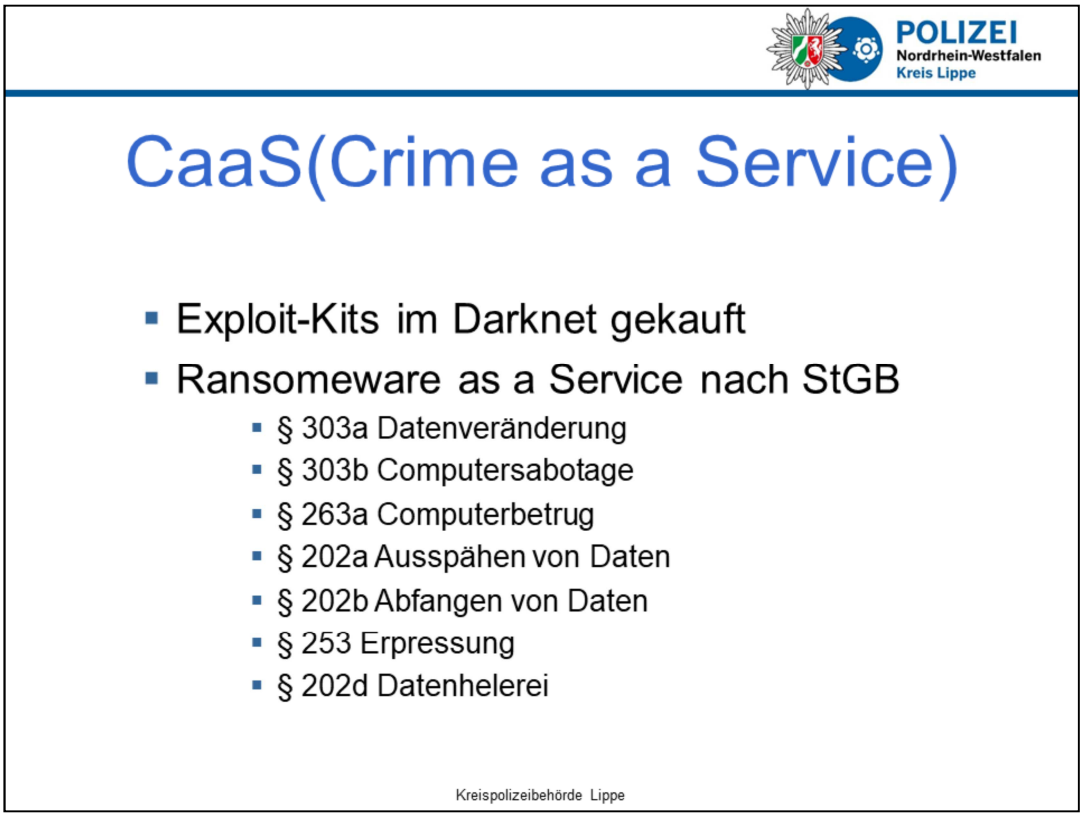
(3) OUTPhase

Negotiator: ist der Unterhändler: vermittelt zwischen den Parteien

Chaser : ist der Verfolger Servicemanager. D.h. wenn nicht in Bitcoin, dann in einen andere Pseudowährung

Money Launderer: Geldwäscher Geldwäsche bezeichnet das Verfahren zur Einschleusung illegal erwirtschafteten Geldes bzw. von illegal erworbenen Vermögenswerten in den legalen Finanz- und Wirtschaftskreislauf

Geldbeträge: 0,4% bis 2% des Jahresumsatzes in Bitcoins werden durchschnittlich verlangt



Verbrechen im Geschäftlichen Umfeld

CaaS (Crime as a Service)

ist eine Ableitung des Begriffs **Software as a Service** (kurz SaaS). Während SaaS als Teilbereich des Cloud Computings davon ausgeht, dass die gesamte IT

oder Teilbereiche bei einem externen IT-Dienstleister betrieben und vom Kunden als Service genutzt werden.

Es werden analog bei **Crime-as-a-Service** von "normalen" Kriminellen die notwendigen Dienste, die sie für ihre Straftat benötigen,
im Internet zusammengekauft.

Exploit Kits (Exploit = Ausbeuter)

->grafische Oberfläche, mit der auch nicht-technische Benutzer anspruchsvolle Angriffe verwalten können.

->So lassen sich Botnetze bauen, DoS-Exploits orchestrieren und Unternehmensdaten stehlen.

->Die Kits werden von professionellen Entwicklern erstellt, diese nutzen zumeist bereits öffentlich bekannte Schwachstellen in Browsern und auf Clients aus. Kommerziell erhältlich sind die Kits unter anderem in

Untergrundforen, die

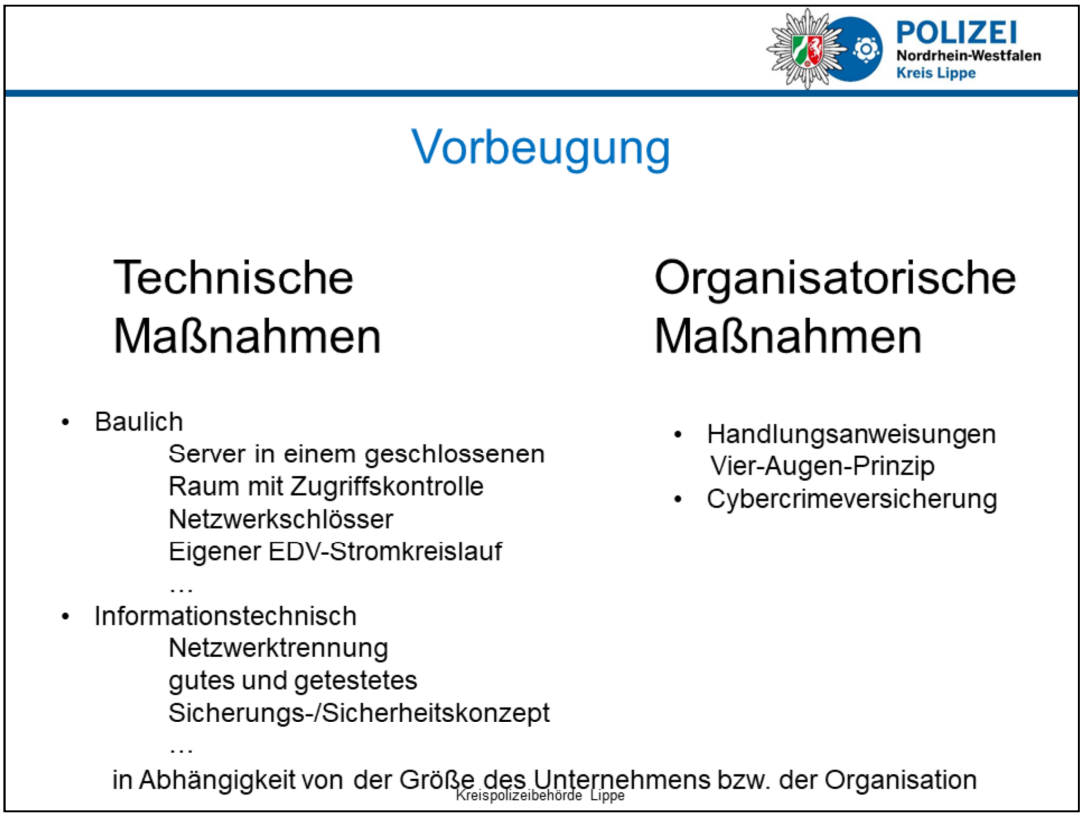
->Preise variieren häufig zwischen drei- und fünfstelligen US-Dollar-Beträgen.

Ein Botnet, auch als Botnetz oder Zombie-Armee bekannt, ist eine Reihe von Computer, die ohne das Wissen ihrer Besitzer dazu verwendet werden,

um Dateien (inklusive Spam und Viren) über das Internet an andere Computer zu senden.

Durch einen **Denial-of-Service (DoS)-Angriff** werden Dienste in ihrer Funktionalität beeinträchtigt und stehen Nutzern sowie Unternehmen nur eingeschränkt zur Verfügung.

Bei **Distributed-Denial-of-Service** greift eine große Zahl von infiltrierten Systemen (manchmal als **Botnet** bezeichnet) ein einzelnes Ziel an.



Aus der DSGVO kennen wir Aus der DSGVO „TOM“

technisch organisatorische Maßnahmen

§ 9 BDSG

Unter **technischen Maßnahmen** sind alle Schutzversuche zu verstehen, die im weitesten Sinne physisch umsetzbar sind, wie etwa

Umzäunung des Geländes

Sicherung von Türen und Fenstern

bauliche Maßnahmen allgemein

Alarmanlagen jeglicher Art

oder Maßnahmen die in Soft- und Hardware umgesetzt werden, wie etwa

Benutzerkonto

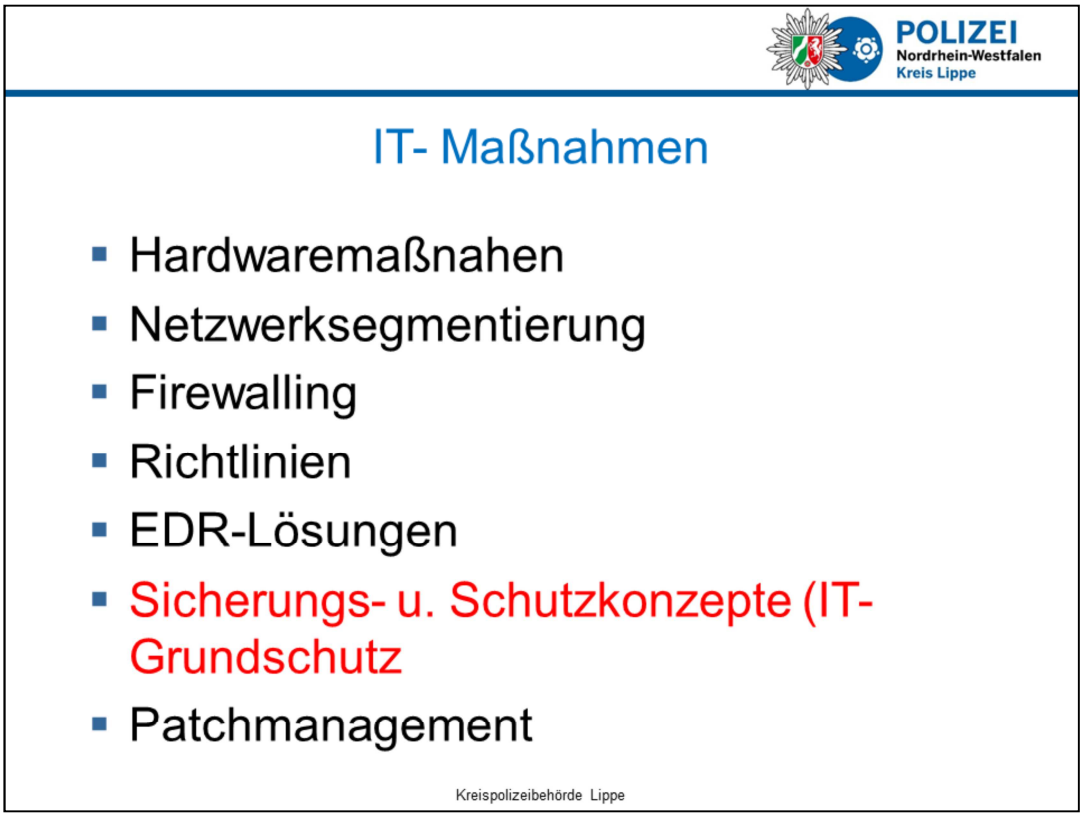
Passworterzwingung,-länge

Logging (Protokolldateien)

biometrische Benutzeridentifikation

Als **organisatorische Maßnahmen** sind solche Schutzversuche zu verstehen die durch Handlungsanweisung, Verfahrens- und Vorgehensweisen umgesetzt werden. Beispiele hierfür sind

Besucheranmeldung
Arbeitsanweisung zum Umgang mit fehlerhaften Druckerzeugnissen
Vier-Augen-Prinzip
festgelegte Intervalle für Stichprobenprüfungen



Netzwerksegmentierung

nach Gebieten und Gerät ….(Werken, Produktion, Verwaltung, Entwicklung, Druckern ….

Firewalling

*Eine Firewall ist ein Sicherungssystem, das ein Rechnernetz oder einen einzelnen Computer vor unerwünschten **Netzwerkzugriffen(von außen nach Innen und Innen nach innen)** schützt. Weiter gefasst ist eine Firewall auch ein Teilaspekt eines Sicherheitskonzepts. Jedes Firewall-Sicherungssystem basiert auf einer Softwarekomponente.

Richtlinien

***Domänencontroller u Gruppenrichtlinien (ADS) Aktive Directory**

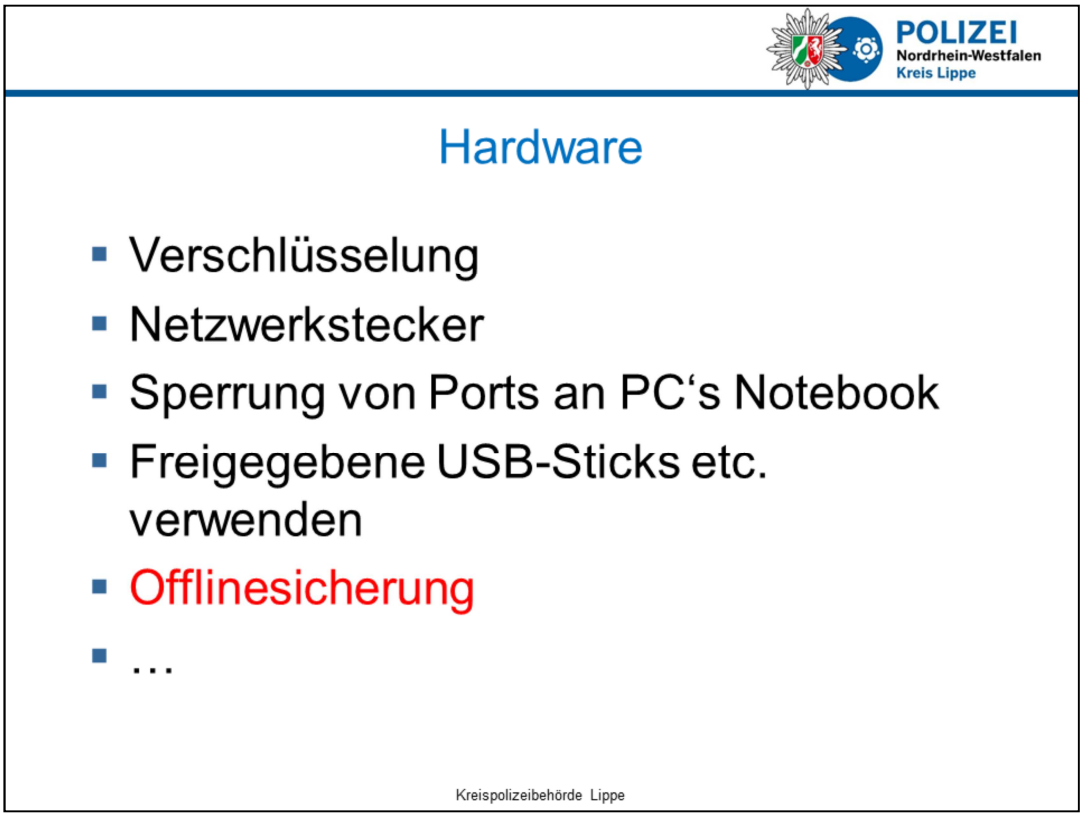
Benutzergruppen

Globale_Gruppen

Sicherheitsgruppen

EDR-Lösungen: Erkennung, Untersuchung und Abwehr von Endgerätebedrohungen – auf dem neuesten Stand

KI-geführte Untersuchungen von Cyberbedrohungen gerade wichtig bei (SaaS)Software as a Service. (Software in der Cloud)



Verschlüsselung von Festplatten und Sticks(Windows 11 wird automatisch verschlüsselt, Hardwarevoraussetzung ist TPM-Chip)

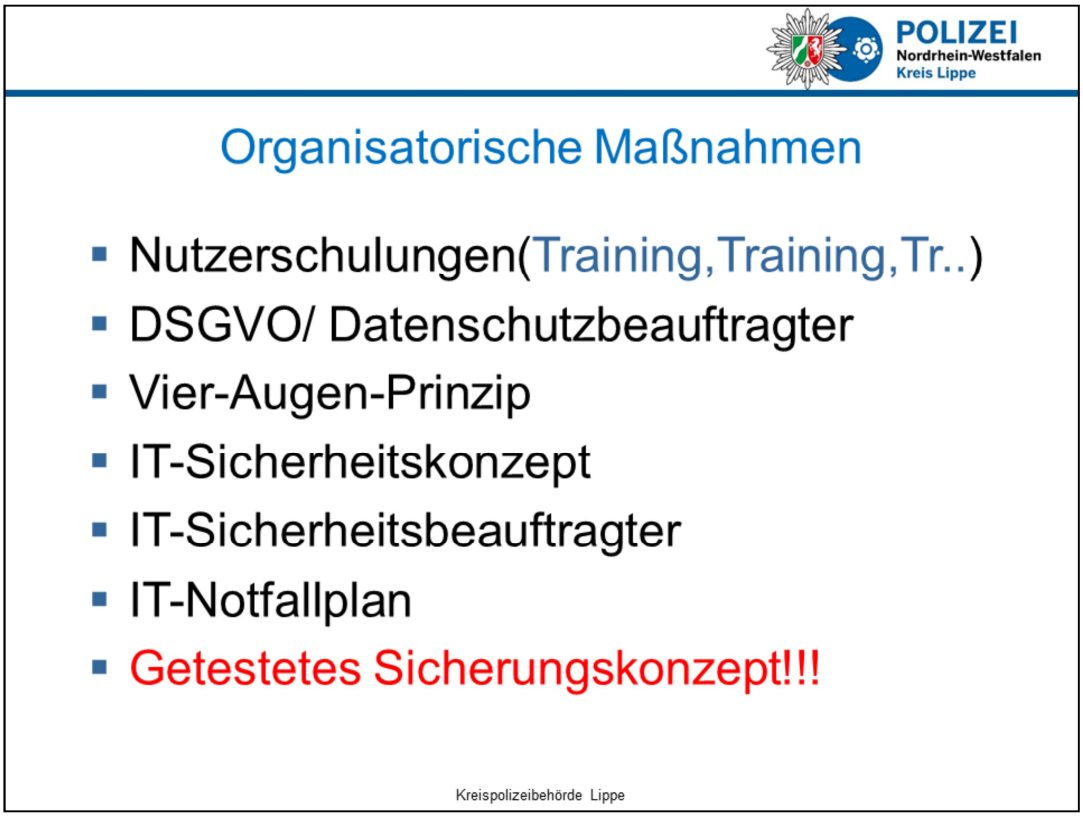
Netzwerksteckerschloss wenn sie nicht gebraucht werden

Softwareverteilung

POLIZEI
Nordrhein-Westfalen
Kreis Lippe

Patchmanagement

- Rechtzeitige Updates
- Desktop Managemant Software
- WSUS-Server
- Test von Updates



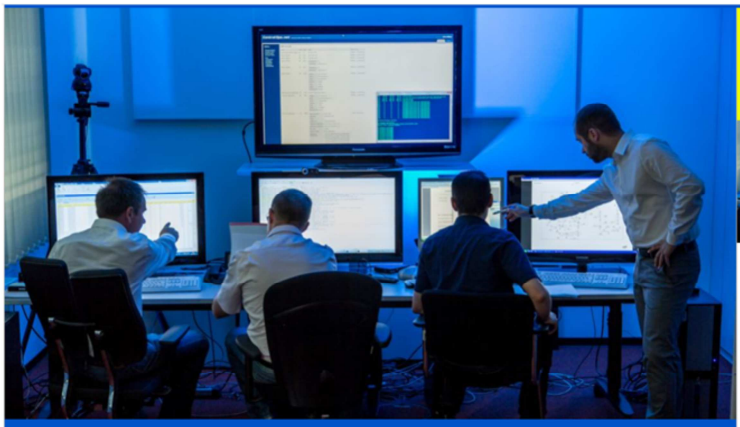
Gerade bei einem Ransomeware-Angriff (Erpressung) ist es wichtig eine externe offline Sicherung von den wichtigsten Systemdaten und Anwendungen zu haben.

Die Sicherungssysteme/-Laufwerke werden oft mit/auch verschlüsselt.

Existenziell: Testen Sie ihr Sicherungskonzept ob die Sicherung eingespielt werden kann!!!

POLIZEI
Nordrhein-Westfalen
Kreis Lippe

Hilfe



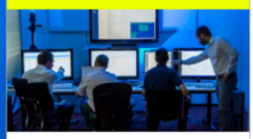
IM NRW / Jochen Tack

Das Cybercrime-Kompetenzzentrum beim LKA NRW

Um der wachsenden Herausforderung dieser Form der Kriminalität adäquat zu begegnen, wurde im Jahr 2011 das Cybercrime-Kompetenzzentrum im Landeskriminalamt Nordrhein Westfalen eingerichtet.

Teilen

KONTAKT FÜR FIRMEN, INSTITUTIONEN UND BEHÖRDEN



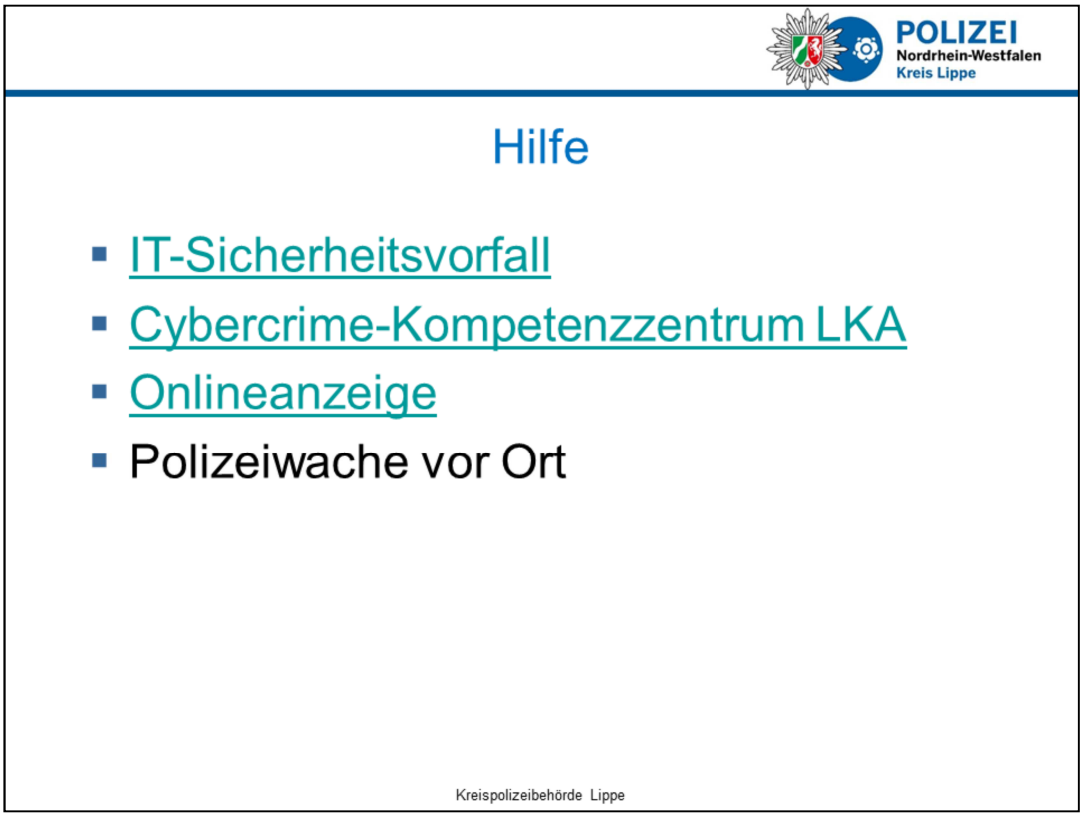
Cybercrime-Kompetenzzentrum
Single Point of Contact (SPoC)

Tel.: +49 211 939-4040
Fax: +49 211 939-194040
E-Mail: cybercrime.lka@polizei.nrw.de

Adresse:
Völklinger Straße 49
40221 Düsseldorf

KONTAKT FÜR BÜRGERINNEN UND BÜRGER

Ihre Polizei vor Ort
Online-Anzeige erstatten



IT-Sicherheitsvorfall LINK: https://www.bsi.bund.de/DE/IT-Sicherheitsvorfall/it-sicherheitsvorfall_node.html

Cybercrime-Kompetenzzentrum beim LKA: https://www.bsi.bund.de/DE/IT-Sicherheitsvorfall/it-sicherheitsvorfall_node.html

Onlineanzeige bei der Polizei: https://polizei.nrw/artikel/anzeige-hinweis