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

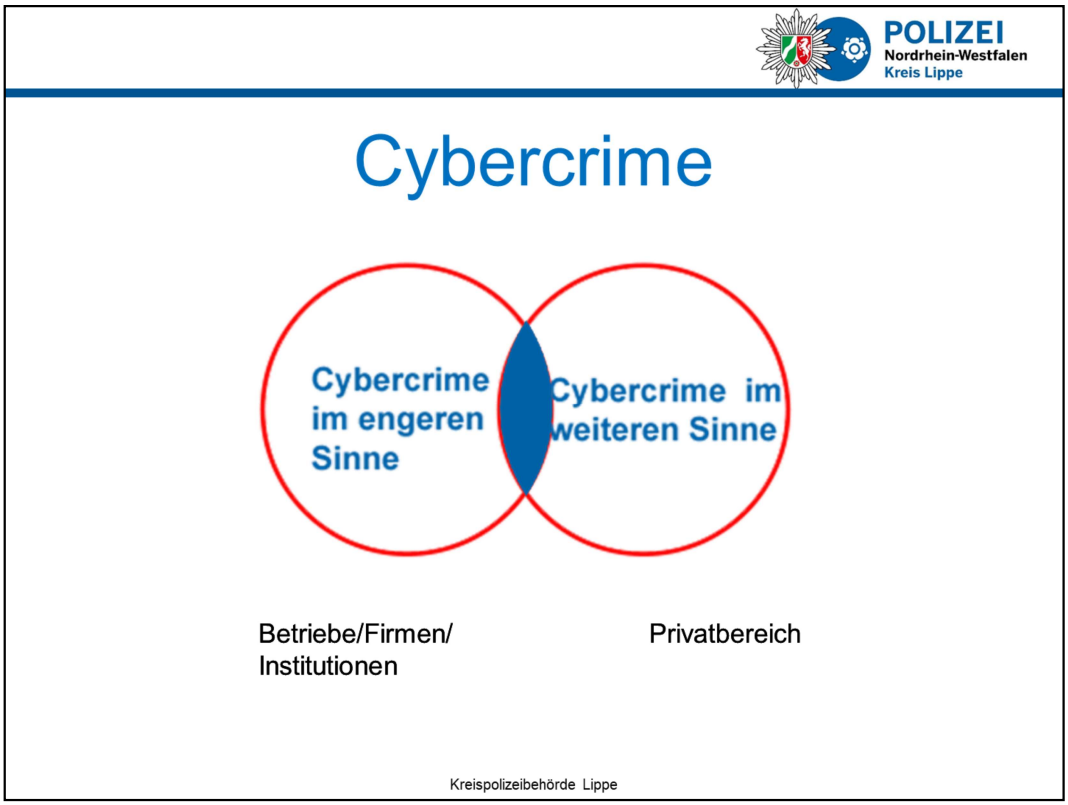
Cybercrime ist Kriminalität unter Nutzung von Informations- und Kommunikationstechnik

Kreispolizeibehörde Lippe

POLIZEI
Nordrhein-Westfalen
Kreis Lippe

Übersicht

- Übersicht Cybercrime und Darknet
- Zahlen und Fakten
- Arten von Cybercrime
- Bedrohungsszenarien
- Angriffsszenarien
- Vorbeugung



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.

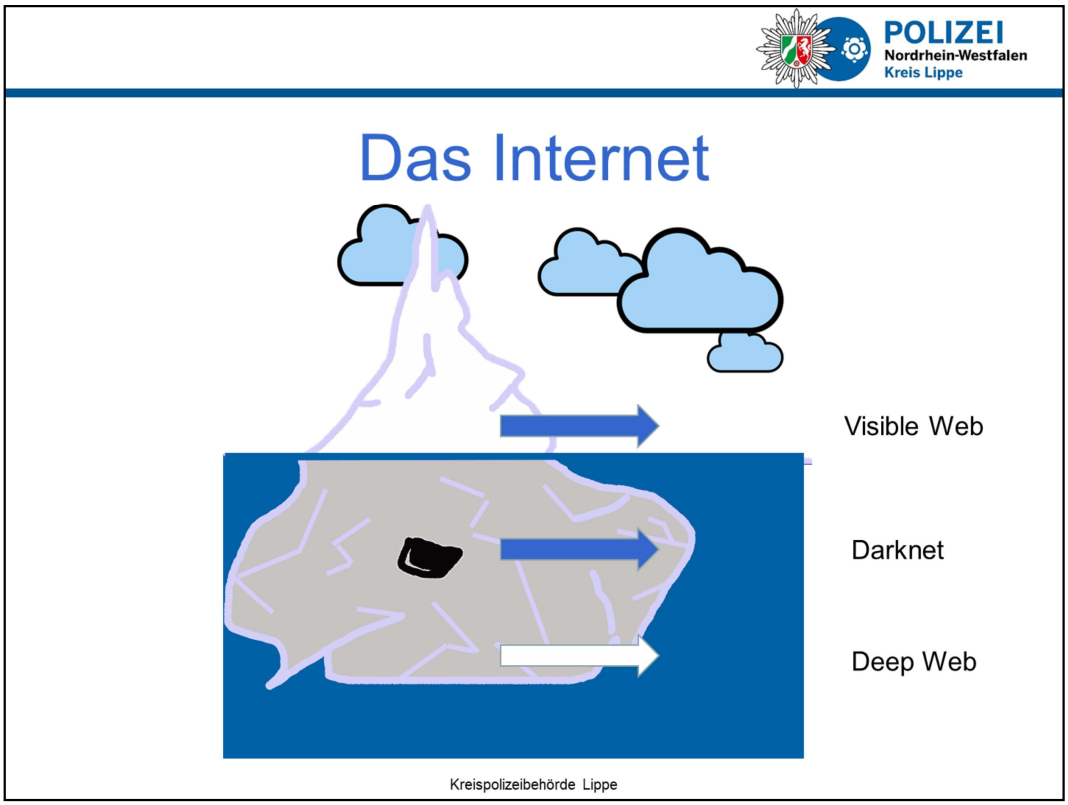
Beispiele: Betrugsdelikte, Kinderpornografie, Cyber-Grooming (Anbahnung) oder Cyber-Mobbing.

Diese Straftaten können praktisch jede Form von Kriminalität annehmen.

Für **Cybermobbing** gibt es keine eigene 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.

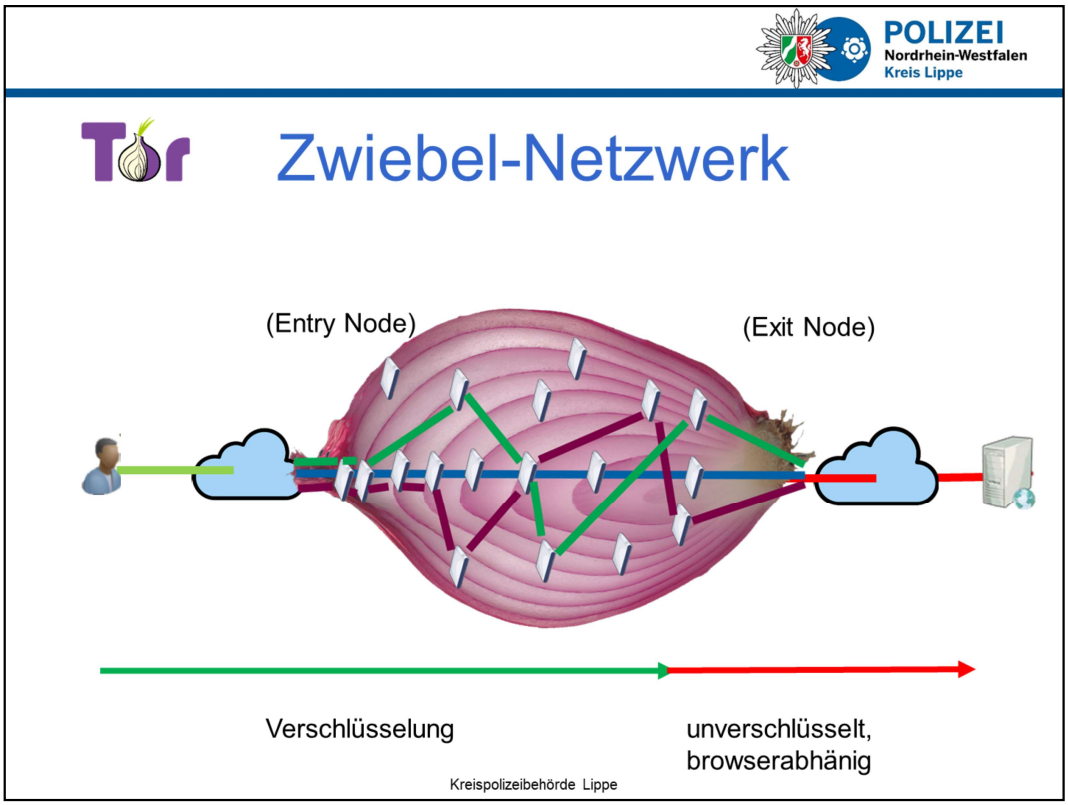


Surface Web, Visible Web oder Clear Net (über Suchmaschinen wie Google zu finden)

Surface = Oberfläche

Deep Web bis zu 500-mal größer ist als das Visible Web

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



Entry Node

Der Weg beginnt immer mit einem Eingangsknoten (Entry Node), mit dem sich der Tor-Client verbindet. Diese Verbindung zwischen Client-Computer und Entry Node ist verschlüsselt.

Da der Entry Node die IP-Adresse des Clients kennt, wird nun der Verkehr zum nächsten Tor-Knoten weitergeleitet. Dieser hat nur auf die IP-Adresse seines Vorgängers Zugriff (Abb. 1). Somit ist die Quell-IP-Adresse des Clients nicht mehr bekannt, wenn der Ausgangsknoten (Exit Node) schließlich das Datenpaket über das Internet anfragt.

Mindestens 3 Roter sind dazwischen.

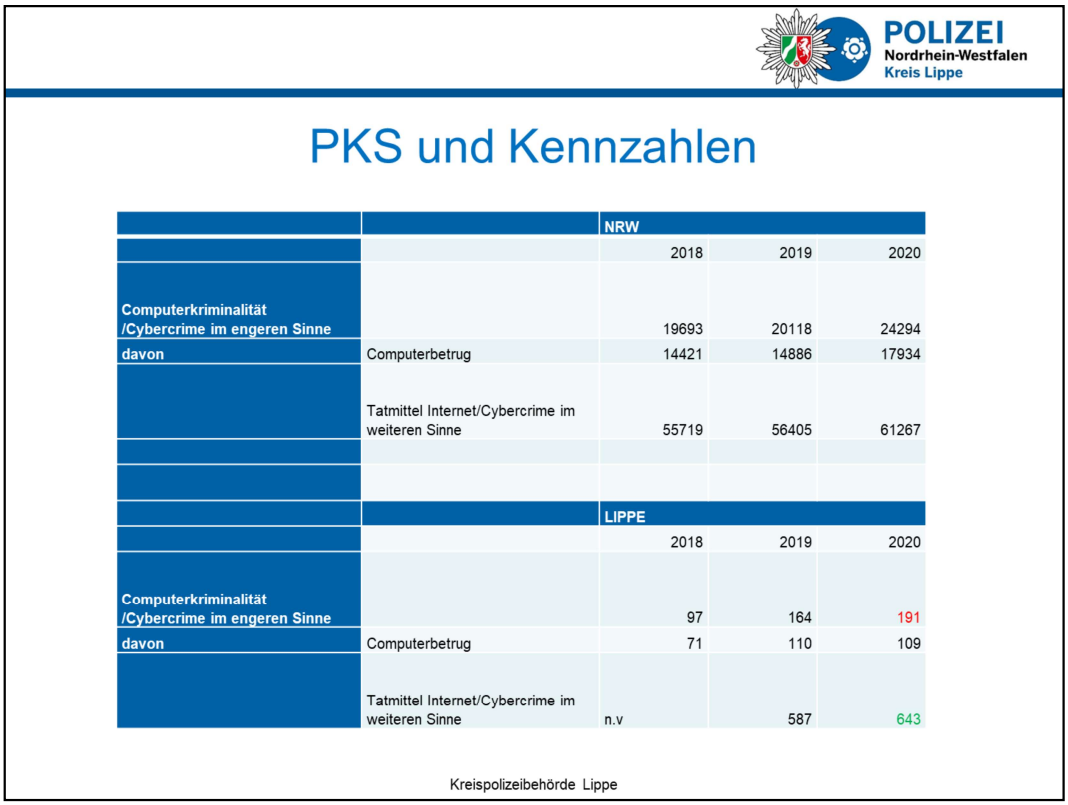
Der Datenverkehr wird also nicht mehr auf der kürzesten Internet-Route transportiert, sondern über das Tor-Netz. Wenn sich nun ein Tor-Ausgangsknoten unter der Kontrolle einer staatlichen Stelle befindet, kann diese den kompletten Verkehr mitschneiden.

Achtung: Vom Client bis zum Ausgangsknoten (Exit Node) ist der Tor-Verkehr zwar verschlüsselt, ab dann hängt es aber vom Browser ab, ob eine SSL/TLS-Verbindung aufgebaut wird.

Endrouter = (Exit Node)

Der Endrouter kann aber auch von einer staatlichen Institution betrieben werden und dann können die Daten mitgelesen werden!!!

Verschlüsselt wird nur innerhalb des Tor-Netzes, nicht zwingend an den Ausgangsknoten Der Webserver (Hostet die Internetseite) kennt nur den Exit Node und nicht „meinen“ Computer.

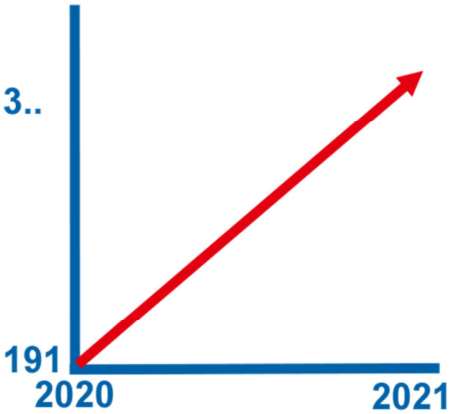


Dies zeigt das Hellfeld(alle bekannten Straftaten), das Dunkelfeld ist noch viel größer.

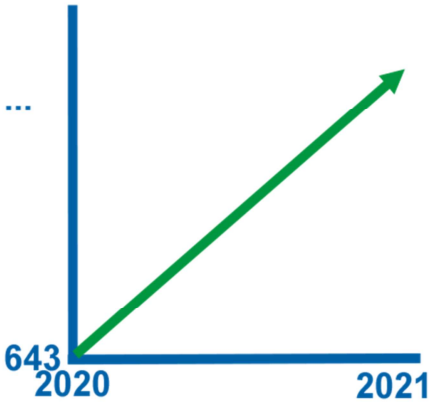
POLIZEI
Nordrhein-Westfalen
Kreis Lippe

Trends in Lippe

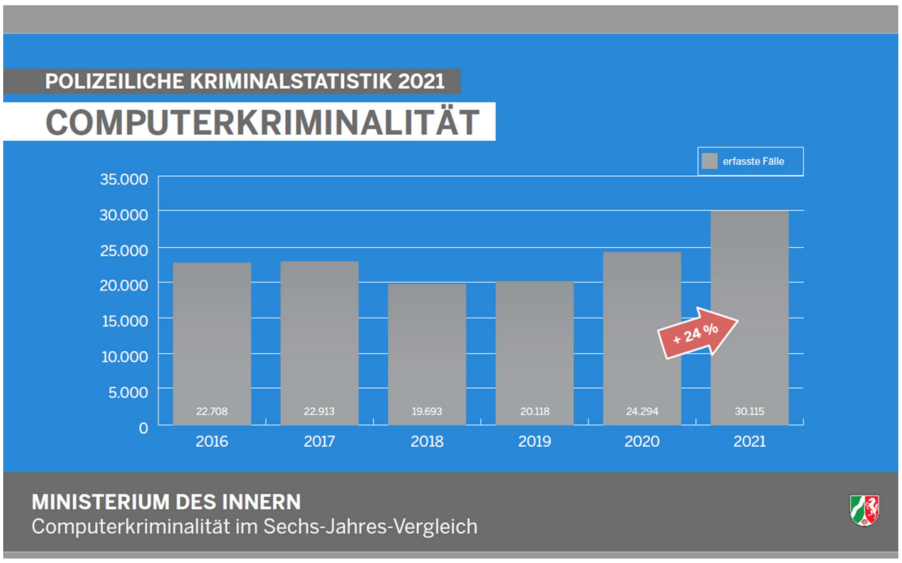
Computerkriminalität



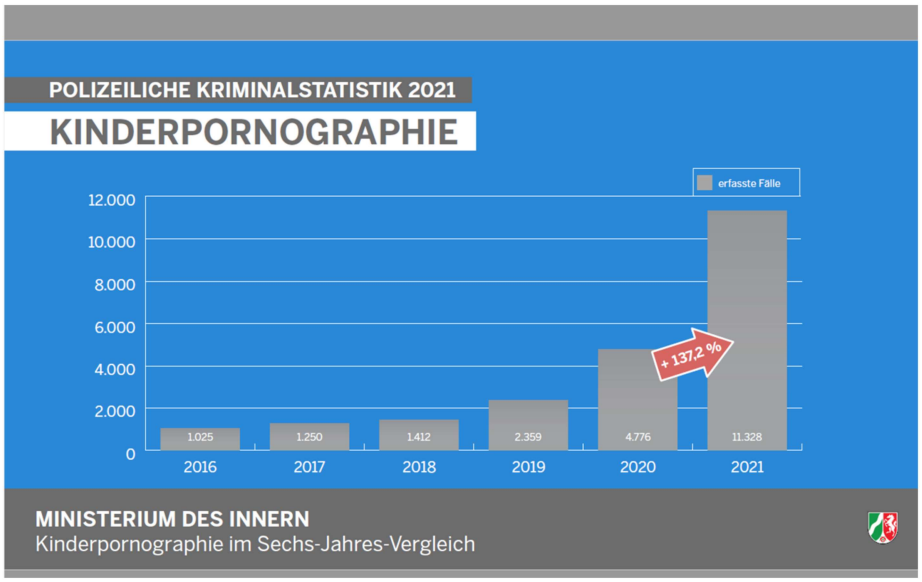
Tatmittel Internet

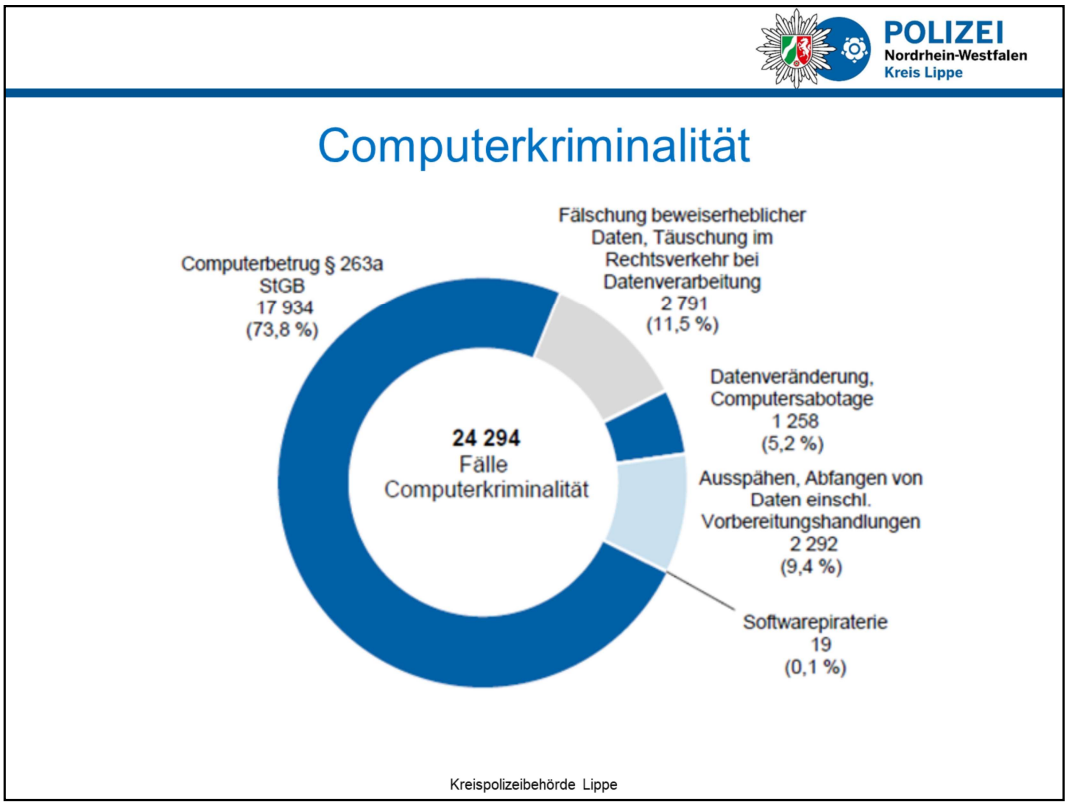


Kreispolizeibehörde Lippe



Kreispolizeibehörde Lippe


POLIZEILICHE KRIMINALSTATISTIK 2021
KINDERPORNOGRAPHIE
erfasste Fälle
12.000
10.000
8.000
6.000
4.000
2.000
0
1.025
1.250
1.412
2.359
4.776
11.328
+ 137,2 %
2016
2017
2018
2019
2020
2021
MINISTERIUM DES INNERN
Kinderpornographie im Sechs-Jahres-Vergleich



§ 263a Computerbetrug Strafgesetzbuch (StGB)

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

*Vermögen des anderen beschädigt

*Beeinflussung von Daten durch Schade Code

*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.

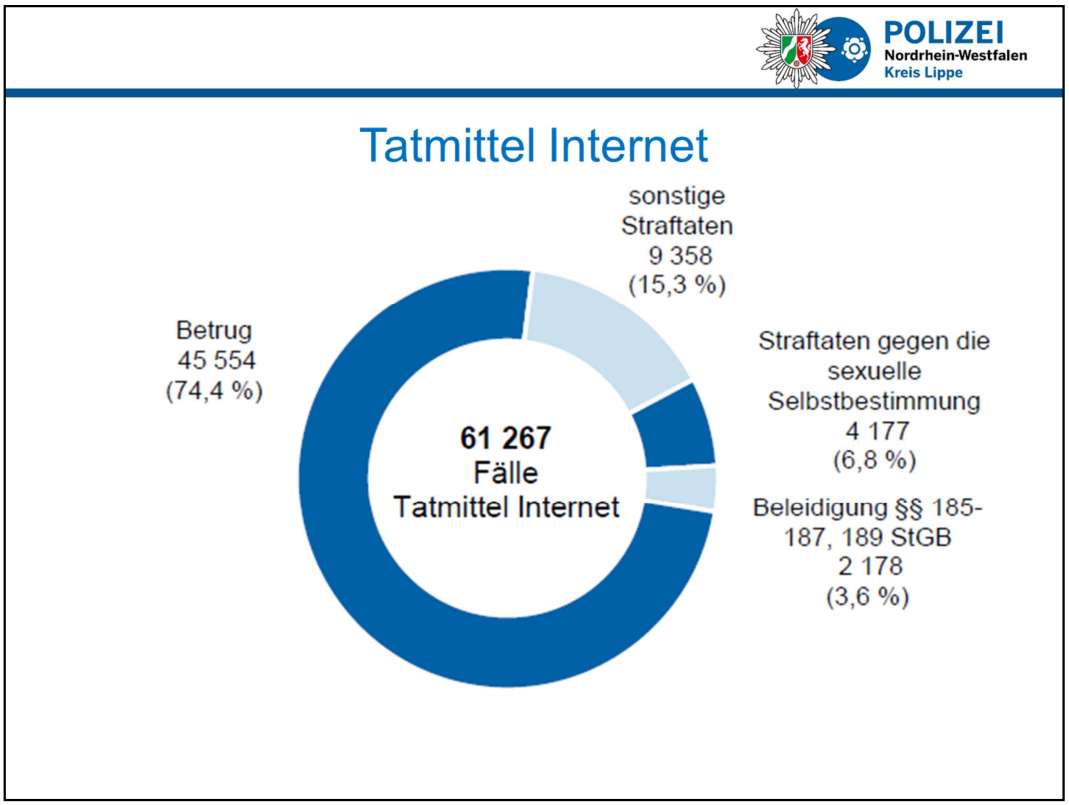
(2) Daten im Sinne des Absatzes 1 sind nur solche, die elektronisch, magnetisch oder sonst nicht unmittelbar wahrnehmbar gespeichert sind oder übermittelt werden.

§ 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

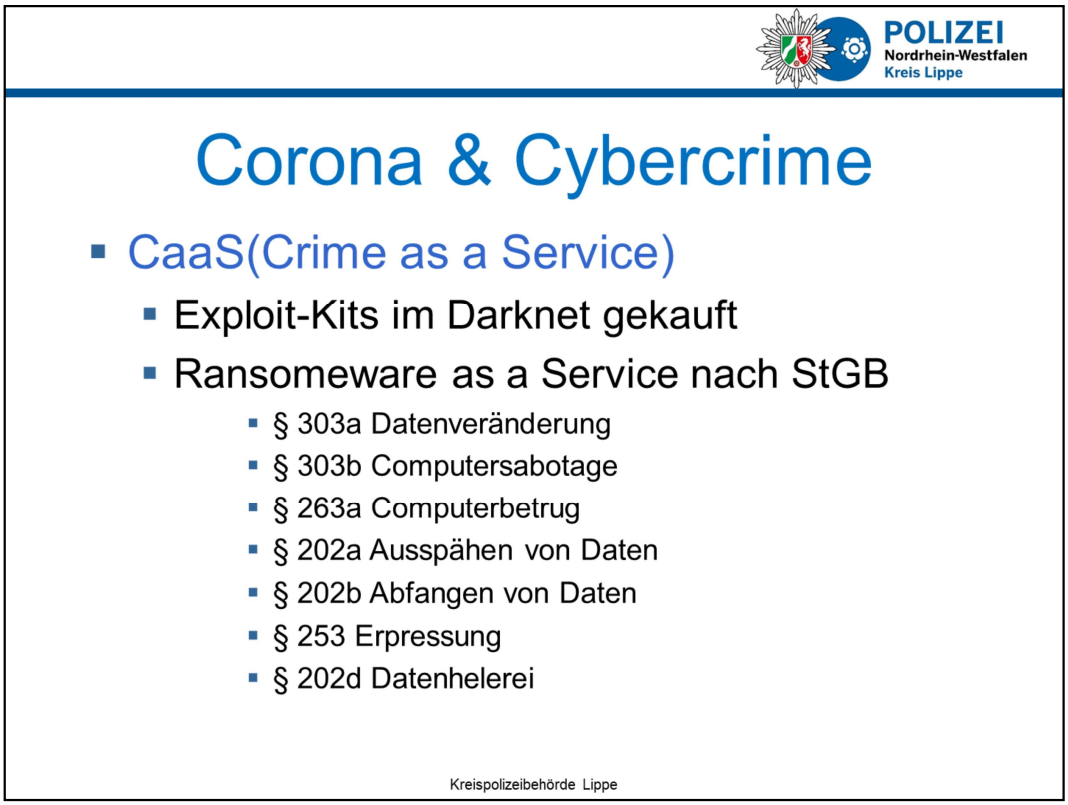
Wer in Beziehung auf einen anderen eine Tatsache behauptet oder verbreitet, welche denselben verächtlich zu machen oder in der öffentlichen Meinung herabzuwürdigen geeignet ist, wird, wenn nicht diese Tatsache erweislich wahr ist, mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe und, wenn die 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.



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

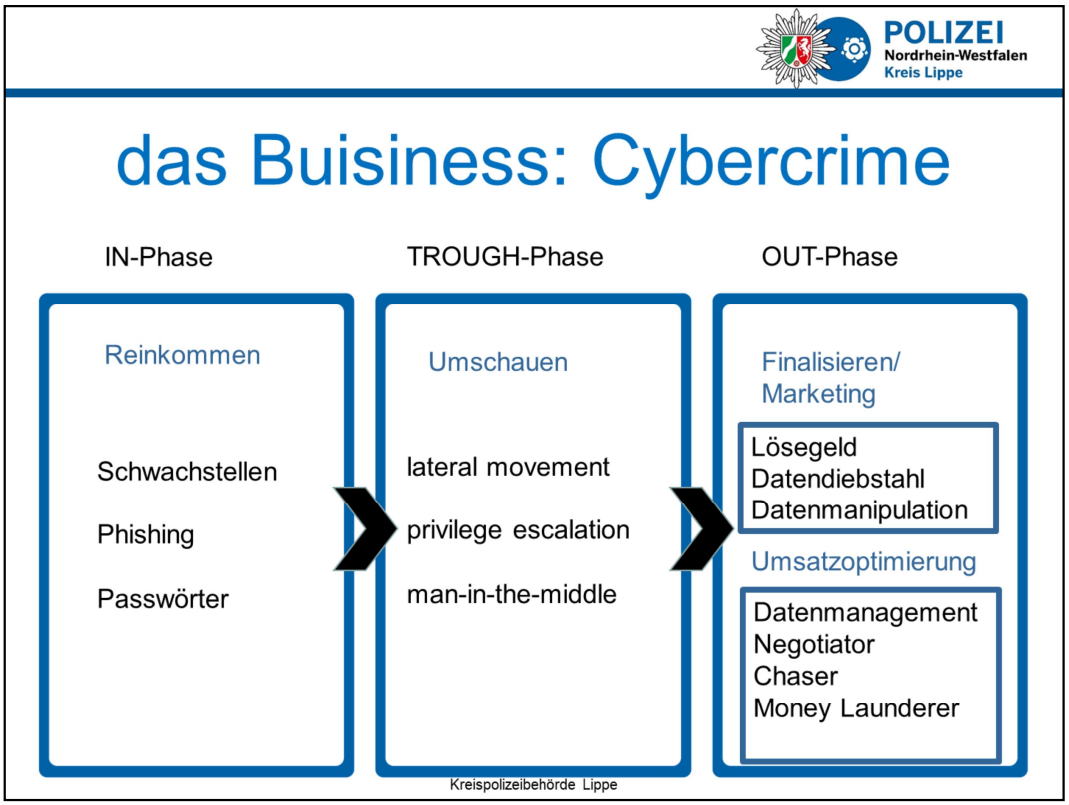
->Preise variieren häufig zwischen drei- und fünfstelligen US-Dollar-Beträgen.

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



Business:

1. **Zufällige Opfer durch Massenangriffe**

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

(1)IN-Phase in das System kommen

Schwachstellen, Phishing, Vishing, Passwörter, Social Engineering,

(2) TROUGH-phase 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

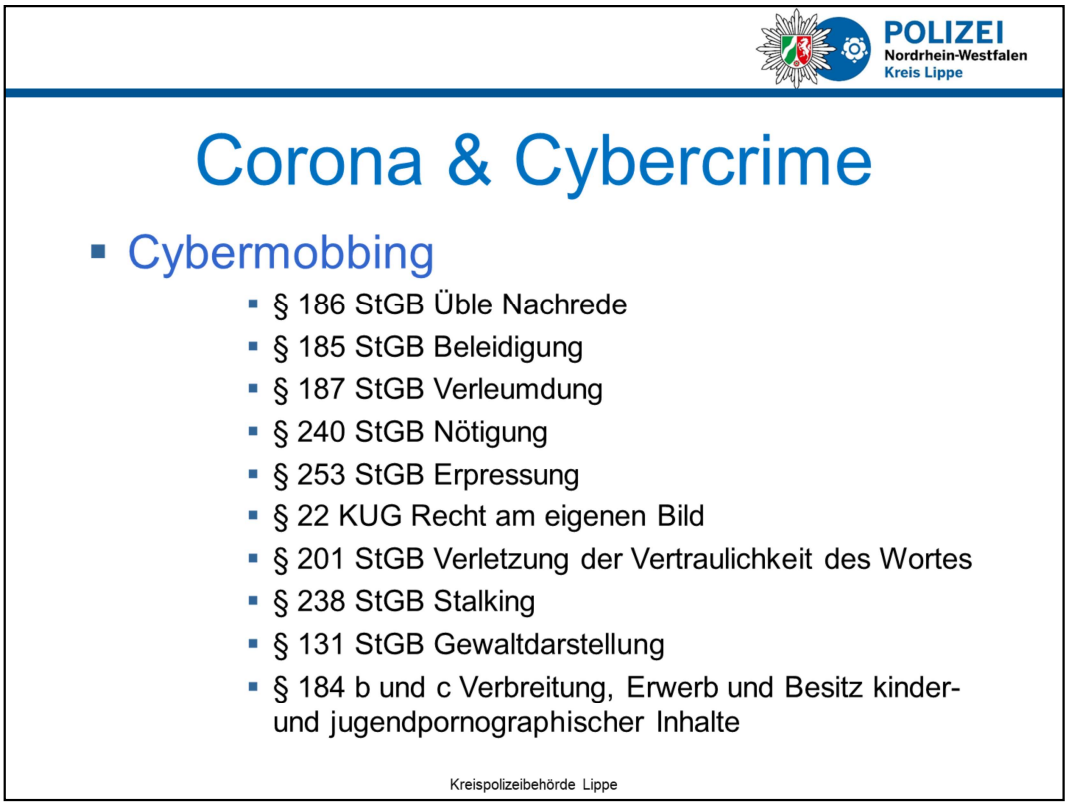
(3) OUT-Phase

Negotiator: ist der Unterhändler: vermittelt zwischen den Parteien

Chaser : ist der Verfolger Servicemanager. D.h. wenn nicht in Bitcoin, dann in einer anderen 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.



Hier sind wir jetzt eher im privaten Bereich und beschäftigen uns mit „herkömmlichen Tatbeständen“

Das Internet wird nur als Werkzeug zur Verbreitung genutzt

Was ist versichert?

Firmen: Ich rede jetzt nicht von Branchenspezifischen Risiken/Angeboten (Angebote werden nach verschieden Kriterien erstellt)

IT-Bedienfehler: Einem deiner Mitarbeiter passiert bei der Bedienung des IT-Systems ein Fehler und er löscht wichtige Kundendaten. Die Daten müssen wiederhergestellt und der Kunde informiert werden, was hohe Kosten und geschädigtes Kundenvertrauen zur Folge haben kann.

Hackerangriff: Deine IT-Infrastruktur wird Opfer eines Hackerangriffs und wichtige Kundendaten geraten in die falschen Hände. Dir und deinen Kunden entstehen finanzielle Schäden, die nun von dir getragen werden müssen.

Ransomware-Angriff: Hacker verschaffen sich Zugang zu einem deiner Server und verschlüsseln wichtige Daten, die nur gegen eine hohe Lösegeldsumme freigegeben werden. Die Daten müssen nun von einem Experten wieder entschlüsselt werden.

Datenrechtsverletzung: Dein Unternehmen verstößt gegen die gesetzlichen Geheimhaltungspflichten der DSGVO. Es entstehen Schadensersatzforderungen.

Wann haftet die Cyberversicherung?

Eigenschäden umfassen alle Schäden – materiell und finanziell –, die einem Betrieb im digitalen Raum entstehen können. Dazu zählen etwa Wiederherstellungskosten von Daten oder IT-Hardware.

Zu den **Haftpflichtschäden** zählen alle Schäden, die ein Unternehmen gegenüber Dritten verursacht. Neben Vermögens- oder Sachschäden sind hier auch immaterielle Schäden (z. B. Persönlichkeitsrechtsverletzung) mit inbegriffen.

Wird ein Betrieb aufgrund eines IT-Schadens für längere Zeit lahmgelegt, entstehen gegebenenfalls Verdienstausfälle. Auch diese **Betriebsausfallschäden** werden von einer Cyber-Versicherung gedeckt.

Privat:

Schutz bei Hackerangriffen

bei Schäden beim Onlinebanking und Onlineshopping. Finanzielle Absicherung bei Betrugsfällen – EU-weit.

Schutz bei Datendiebstahl

von privaten Online-Konten. Kostenübernahme beim Missbrauch persönlicher Daten.

Schutz bei Cybermobbing

Juristische und psychologische Expertenberatung sowie Löschung rufschädigender Inhalte.

Reputationsschutz

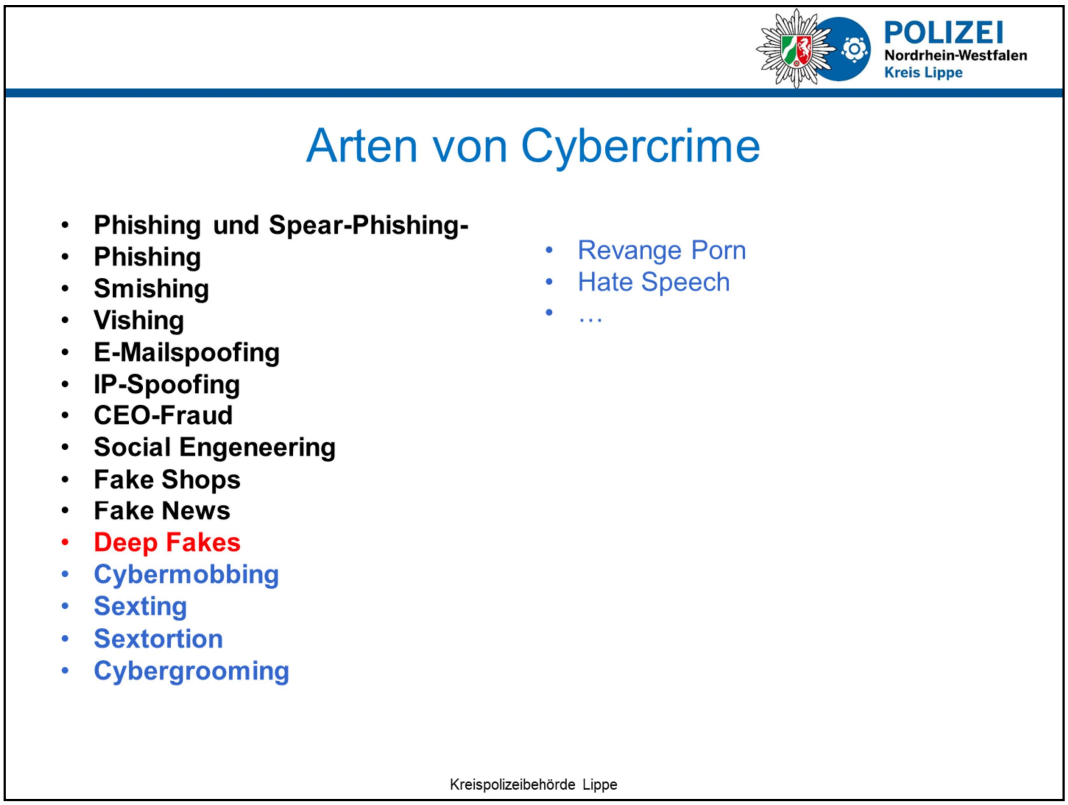
hilft, wenn gegen Ihren Willen persönliche Daten im Internet veröffentlicht oder missbräuchlich verwendet wurden.

Hardware- und Software-Schutz

Kostenübernahme bei Software-Verlust und Hardware-Fehlern nach Cyberattacken.

Smart-Home-Schutz

Übernahme von Energie-Mehrkosten und Reparaturkosten nach Cyberattacken.



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

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

Spearphishing direktes Ausspähen z.B. 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.

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

CEO-Fraud Schreiben von wahrheitsähnlichen E-Mails an Menschen mit Faktura. (z.B. vom CEO)

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.

Fake Shops sind gefälschte Shops die anderen zum Verwechseln ähnlich sind.

Fake News Falschmeldungen erstellen und streuen mit dem Ziel der Beeinflussung.

Deep Fakes: beschreiben realistisch wirkende Medieninhalte, welche durch Techniken der künstlichen Intelligenz abgeändert und verfälscht worden sind.

Cybermobbing ist Mobbing über das Internet. (Straftatbestände siehe Folie 15)

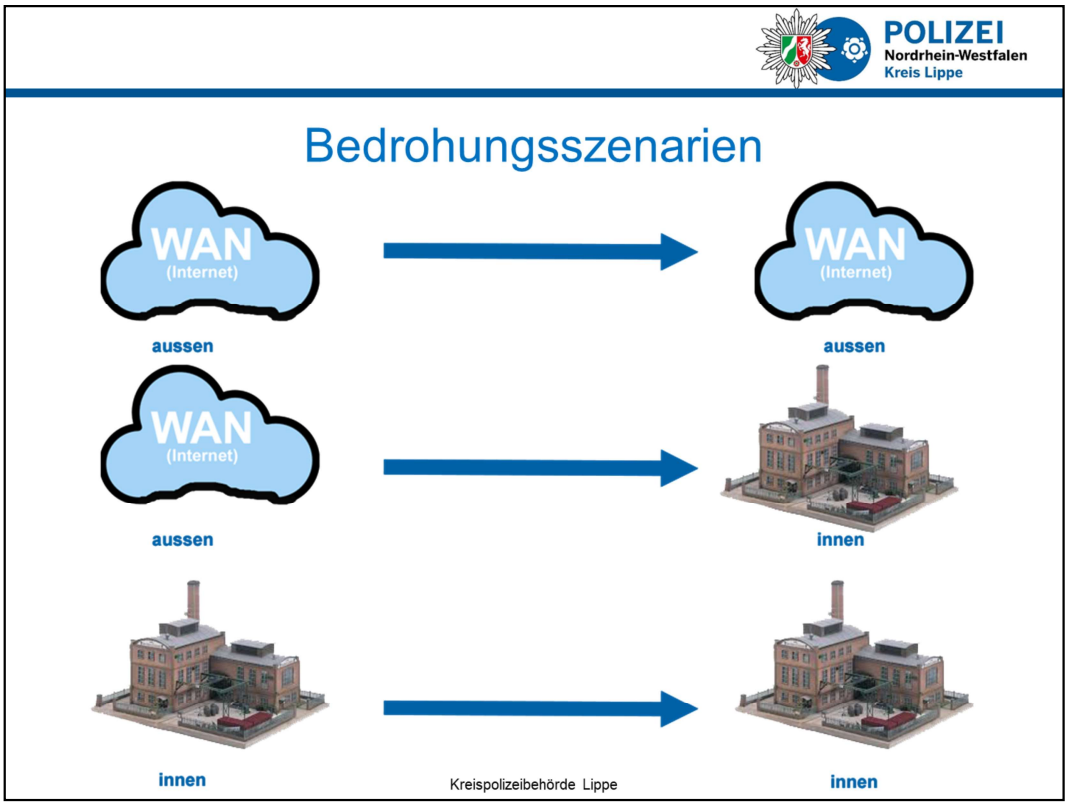
Sexting: Eine Mischung aus SMS und Texten per Messanger.

Sextortion Erpressung aufgrund von Bildern etc. ist die Androhung, intime Informationen über das Opfer zu veröffentlichen, es sei denn, das Opfer zahlt dem Täter Geld.

Cybergrooming ist die Anbahnung von Kontakten meistens zu Kindern und Jugendlichen.

Revange Porn bezeichnet aus Rache versende Bilder und Videos mit sexuellen Inhalten.

Hate Speech versteht man zumeist verbale Angriffe auf Personen oder Gruppen aufgrund bestimmter Attribute wie Hautfarbe, Herkunft, Geschlecht, sexuelle Neigungen.



Beispiele:

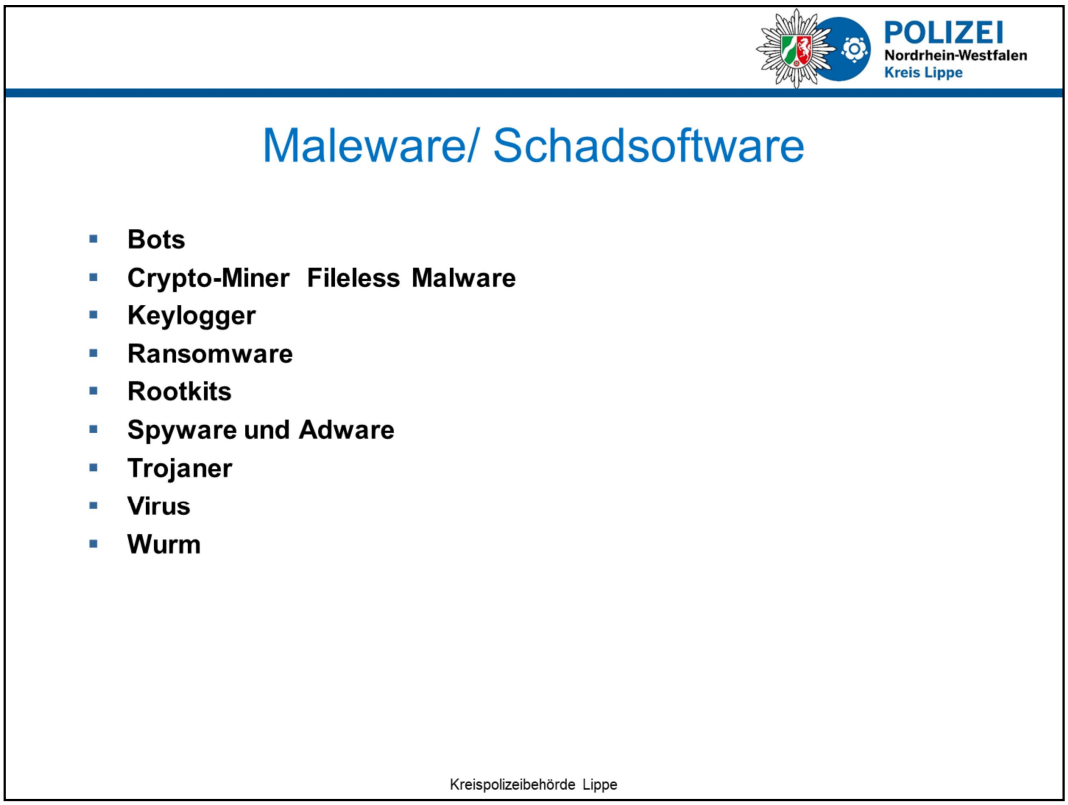
(1) DDos Angriff (Distributed Denial of Services) Nichtverfügbarkeit eines Dienstes oder Servers gezielt herbei. Website-.Mail etc.

*man-in-the-middle-Angriffe bei Schlecht geschützten Zertifikaten (Daten werden gelesen) Verschlüsselung wird ausgesetzt

*Hacking über sogenannte Bots um Passwörter zu knacken

(2) Ein Versuch in das System einzudringen über E-Mail, offenen Ports etc.

(3) Eingeschmuggelte Programme sogenannte Spyware arbeitet im Hintergrund oder es wir sabotiert



Bots DDoS-Angriffe durch ein Botnetz. Netz aus übernommenen Computern.

Crypto-Miner Computer werden übernommen um Cyberwährung zu generieren.

Fileless Malware Programme die sich im Arbeitsspeicher festsetzen.

Keylogger Tastatureingaben aufzuzeichnen.

Ransomware Erpressung und Verschlüsselung.

Rootkits Softwarewerkzeuge, die einen langfristigen (Fern-)Zugang zu Computersystemen ermöglichen sollen, sind Trojanern sehr ähnlich und halten die

Tür zum Nachladen von Viren, Würmern, etc. frei.

Spyware und Adware spioniert das Verhalten oder den Computer der Nutzer aus. Dies schließt das Surfverhalten, die Tastaturanschläge oder auch Anmeldedaten für Nutzerkonten ein.

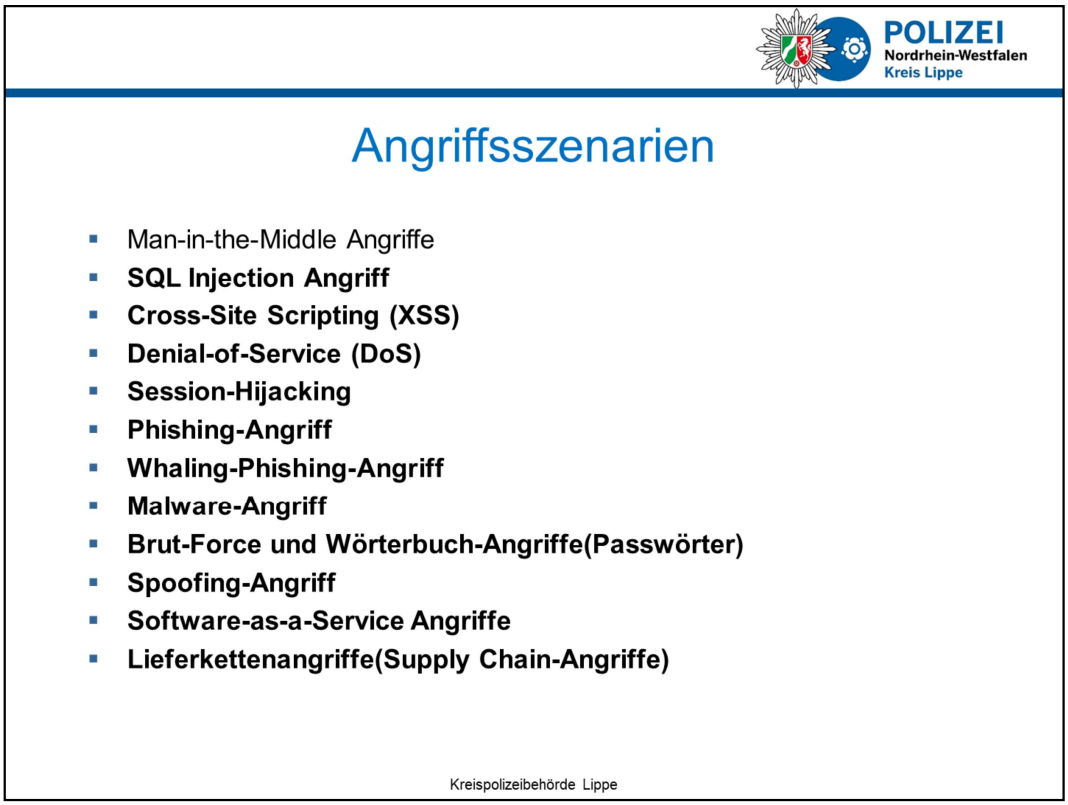
Erstellt auch neue Profile.

Trojaner Programmteile, die sich in erwünschten, nützlichen Programmen verstecken, können Backdoors offenhalten.

Virus Computerprogramm, das Kopien von sich selbst in Programme, Dokumente oder Datenträger schreibt. Verändert bestimmte Dateien dabei so, dass es beim Starten des Wirtsprogramms mitausgeführt.

Wurm versuchen Würmer selbstständig, sich zu verbreiten und neue Systeme zu befallen Trojan-Banker, Trojan-SMS oder Trojan-Dropper. Letztere versuchen, Viren auf den betroffenen Systemen zu installieren oder die Erkennung von Schadprogrammen zu verhindern.

Drive-by-Download, Drive-by-Exploits beziehen sich jeweils auf den unbeabsichtigten Download von Computersoftware aus dem Internet. Dazu zählen Downloads, die eine Person durch Klicken autorisiert hat, aber auch Downloads, die ohne das Wissen einer Person z.B. durch Malware geschehen.



Whaling-Phishing-Angriff auf einen Wal in diesem Fall jemand in der Chefetage. (Großer Fisch)

Man-in-the-Middle Angriffe:

Bei einem Man-in-the-Middle-Angriff platziert sich der Angreifer logisch oder physisch zwischen dem Opfer und den verwendeten Ressourcen.

Er ist dadurch in der Lage, die Kommunikation abzufangen, mitzulesen oder zu manipulieren. Die Ende-zu-Ende-Verschlüsselung ist eine wirksame Gegenmaßnahme gegen eine Man-in-the-Middle-Attacke.

SQL Injection Angriff:

SQL-Injection ist das Ausnutzen einer Sicherheitslücke in Zusammenhang mit SQL-Datenbanken. Die Sicherheitslücke entsteht durch einen Programmierfehler in einem

Programm, das auf die Datenbank zugreift.

Cross-Site Scripting (XSS):

Cross-Site-Scripting bezeichnet das Ausnutzen einer Computersicherheitslücke in Webanwendungen, indem Informationen aus einem Kontext, in dem sie nicht vertrauenswürdig sind, in einen anderen Kontext eingefügt werden, in dem sie als vertrauenswürdig eingestuft werden.

Denial-of-Service (DoS):

Denial of Service bezeichnet in der Informationstechnik die Nichtverfügbarkeit eines Internetdienstes, der eigentlich verfügbar sein sollte. Häufigster Grund ist die Überlastung des Datennetzes.

Session-Hijacking: Session und Sicherheit

Beim Session-Hijacking wird eine gültige Session von einem Angreifer entführt (daher das Hijacking). Nach erfolgreicher Entführung kann der Angreifer im schlimmsten Fall die Identität des Nutzers übernehmen und die Anwendung in dessen Namen nutzen.

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.

Malware-Angriff: Ein Malware-Angriff ist ein geläufiger Cyberangriff, bei

dem **Malware** (normalerweise bösartige Software) unbefugte Aktionen im System des Opfers ausführt.

Brut-Force und Wörterbuch-Angriffe (Passwörter): Aus dem Englischen übersetzt-In der Kryptographie besteht ein Brute-Force-Angriff darin, dass ein Angreifer viele Passwörter oder Passphrasen eingibt, in der Hoffnung, irgendwann richtig zu raten. Der Angreifer überprüft systematisch alle möglichen Passwörter und Passphrasen, bis das richtige gefunden wird.

Spoofing-Angriff: Spoofing ist der Akt der Verschleierung einer Kommunikation oder einer Identität, damit sie mit einer vertrauten, autorisierten Quelle in Verbindung gesetzt wird.

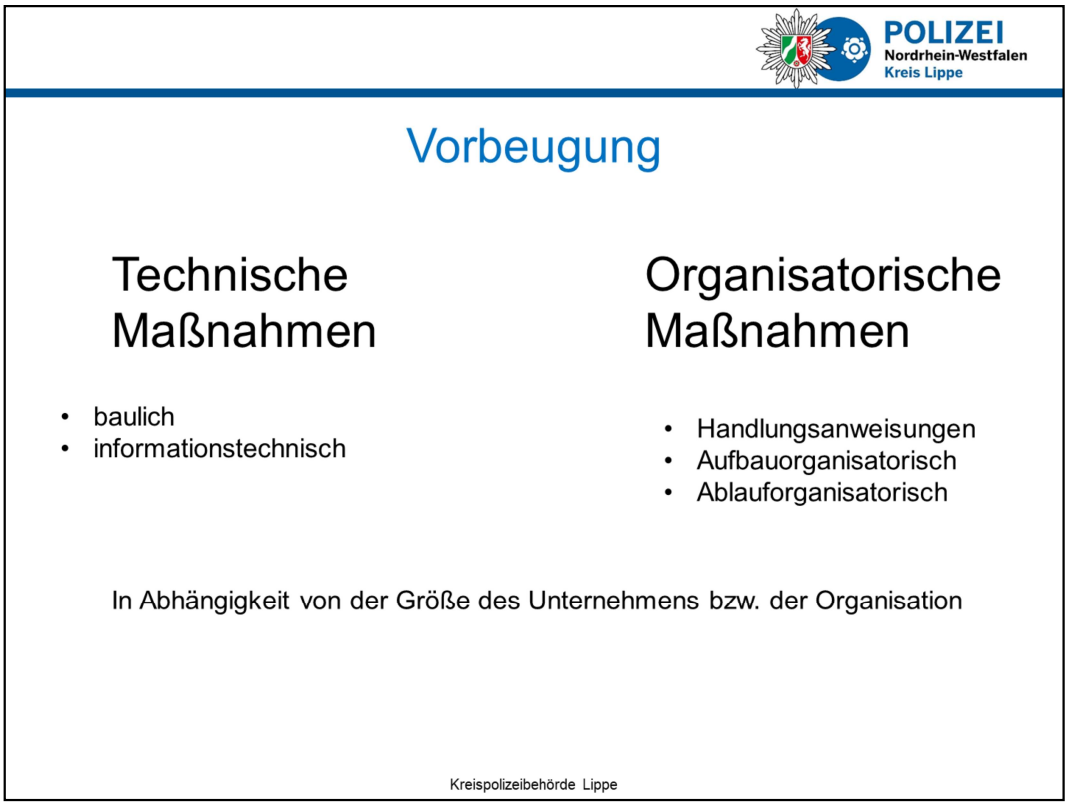
IP-Spoofing

Websitespoofing

Telefonspoofing

Software-as-a-Service Angriffe: Bei „Software als Service“, kurz SaaS (Software as a Service), verwenden Sie **bereitgestellte Software**, die Sie nicht lokal installiert haben, sondern über eine **Internetverbindung** benutzen. Hard- und Software werden dabei vom Anbieter der Dienstleistung gestellt. Ist diese Software befallen, so kann ihr System oder ihre Daten ausspioniert oder befallen werden.

Lieferkettenangriffe(Supply Chain-Angriffe): Der Begriff Supply-Chain-Attacke meint Angriffsszenarien, bei denen Cyberkriminelle in den Herstellungsprozess, beziehungsweise den Entwicklungslebenszyklus eingreifen oder ihn kapern, so dass mehrere Endverbraucher des fertigen Produkts oder Dienstes nachteilig beeinflusst werden.



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

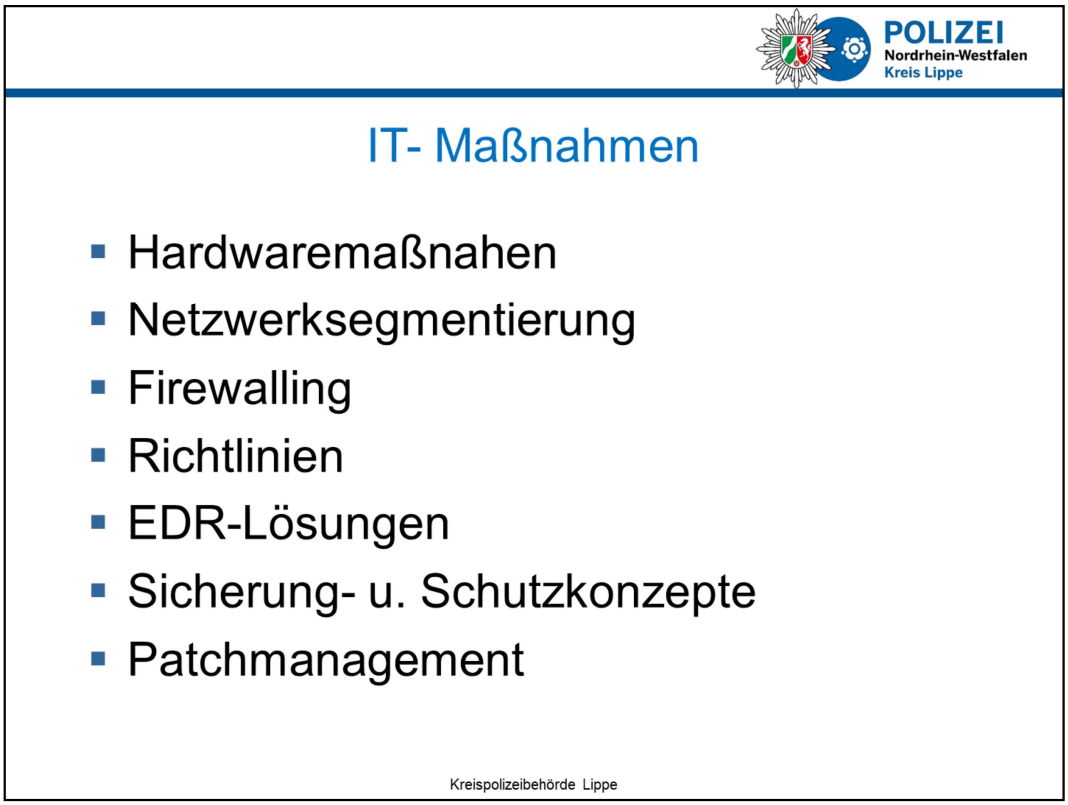
- Besucheranmeldung
- Arbeitsanweisung zum Umgang mit fehlerhaften Druckerzeugnissen
- Vier-Augen-Prinzip
- festgelegte Intervalle zur Stichprobenprüfungen

POLIZEI
Nordrhein-Westfalen
Kreis Lippe

Technische Maßnahmen/baulich

- Zugriffskontrolle für den Server/-raum
- Netzwerkschlösser
- Eigener EDV-Kreislauf(Strom)
- …

Problem der Sabotage



Netzwerksegmentierung

*Gebieten und Gerät ….

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 Direktory**

Benutzergruppen

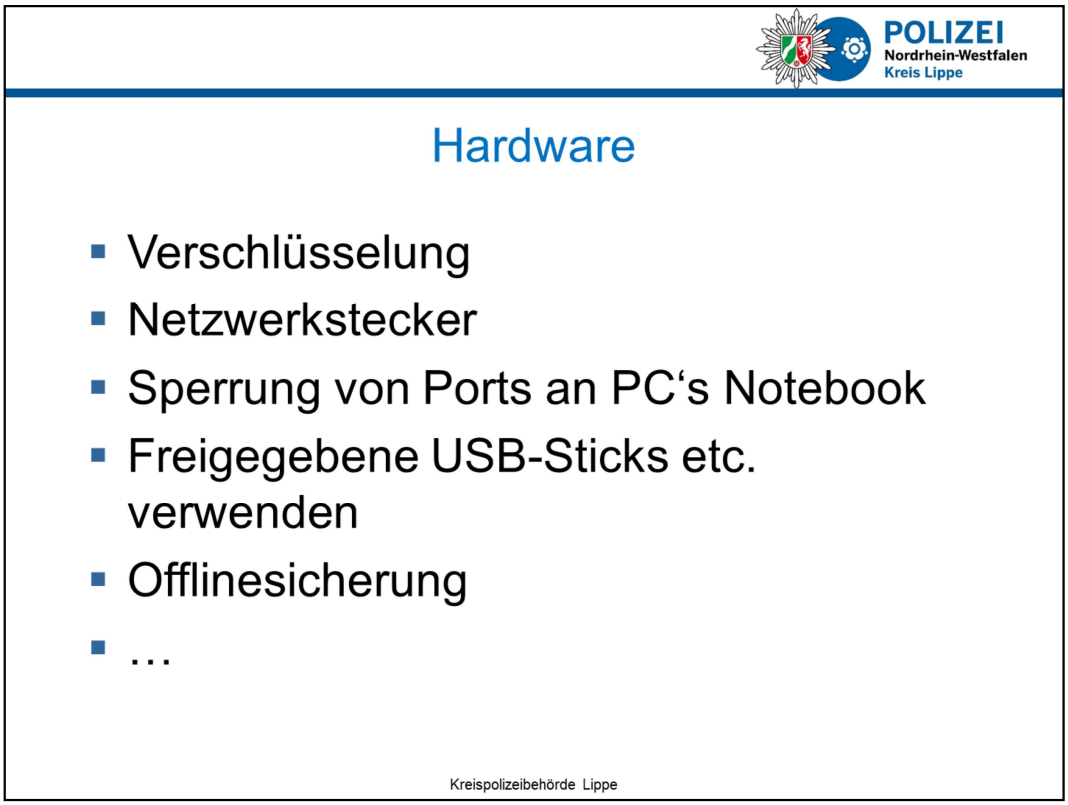
Globale_Gruppen

Sicherheitsgruppen

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

KI-geführte Untersuchungen von Cyberbedrohungen gerade wichtig bei

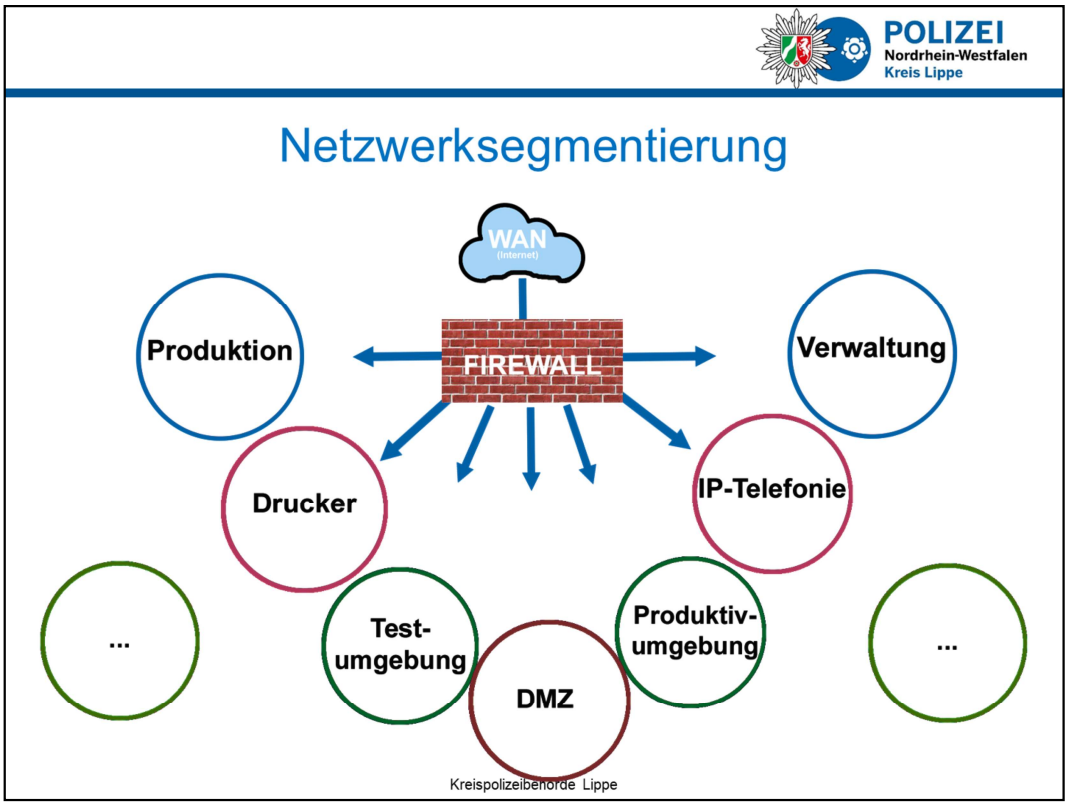
(SaaS)Software as a Service. Software in der Cloud



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

Netzwerksteckerschloss wenn sie nicht gebraucht werden

Softwareverteilung



90% der Angriffe gehen auf Windowsumgebungen zurück (ADS_Umgebung)

Firewall: **Stateful und Stateless Firewalls?**

Stateful Firewall = Datenpakete werden während der ganzen Übertragung miteinander verglichen, in eine Zwischentabelle gespeichert und auf evtl. Angriffe wie DDos-Attacken kontrolliert

Die Übertragung wird evtl. abgebrochen

Header und Inhalt der Pakete **ist dynamisch**

Stateless Firewalls = Paketfilter-Firewalls bezeichnet aber nur Header von Paketen **basiert auf festgelegten Regeln** Traffic Kontrolle und auf Portnummern oder Zieladressen basieren

Netzwerksegmentierung

durch eine ordentliche Netzwerksegmentierung auch eine Funktionstrennung einführen

Funktionstrennung nach

*__Gebieten__ (Admin-PC sowie der Shop-Server einzeln),

Online-Shop und die Datenbank

Produktion od. Verwaltung

*__Geräteart__

IP-Telefonie

, Drucker,

Server

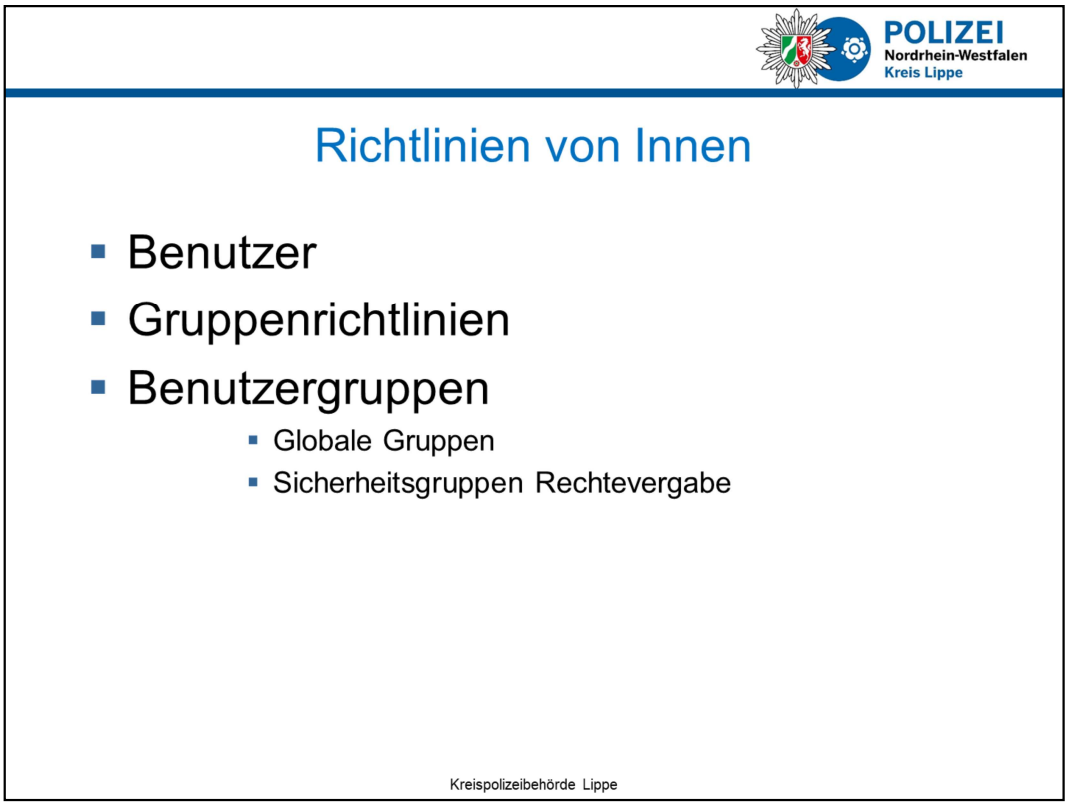
***Testumgebung u. Produktivumgebung**

***Demilitarisierte Zone (DMS)** als Puffer zwischen Ihrem internen Netzwerk

*Webserver mit dem öffentlichen Internetauftritt Ihres Unternehmens,

*öffentlich erreichbare Mailserver oder ein

Proxyserver für den Internetzugang der Mitarbeiter.



Benutzer: Administratoren, Domänenadmins, lokale Admins etc.

Gruppenrichtlinien: Über Domäne und Active Direcory z.B.: Passwortrichtlinien die auf Gruppen bzw. Organisationseinheiten angewendet werden können.

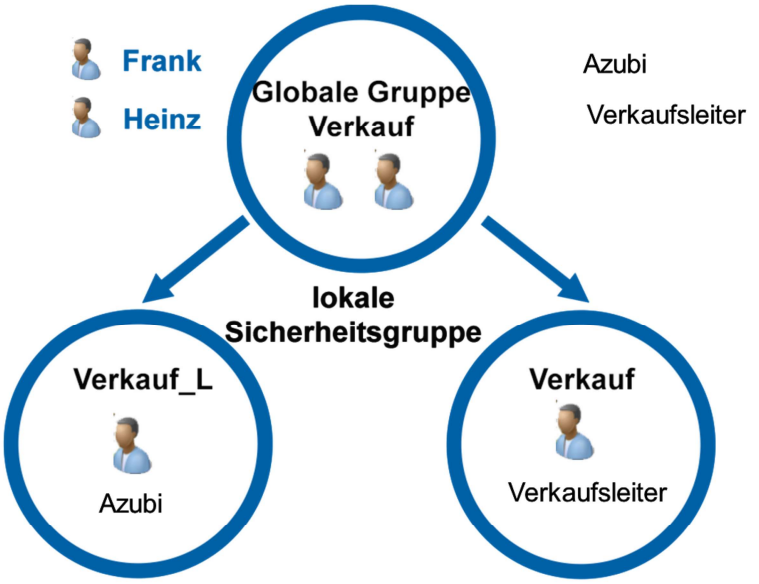
Benutzergruppen:

Globale Gruppen: (Auftragsbearbeitung, Vertrieb, …

Lokale_Sicherheitsgruppen: Auftragsbearbeitung_R (read), Auftragsbesrbeitung_AE (Lesen, Schreiben, Ändern)

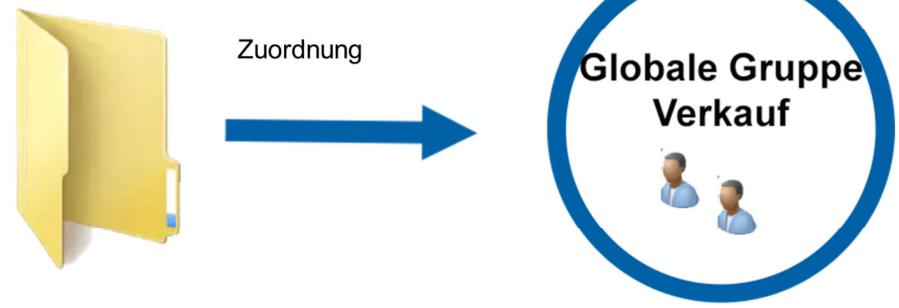
POLIZEI
Nordrhein-Westfalen
Kreis Lippe

Benutzer und Gruppen



POLIZEI
Nordrhein-Westfalen
Kreis Lippe

Benutzer und Gruppen



Absatzzahlen

den meisten Fällen als ausreichend betrachtet werden kann und daher die wesentlich teurere Risikoanalyse ersetzt. In Fällen eines höheren Sicherheitsbedarfs kann der IT-Grundschutz als Grundlage für weitergehende Maßnahmen genutzt werden.

Die ursprüngliche Zertifizierung nach *IT-Grundschutz* wurde durch eine anerkannte *ISO/IEC 27001-Zertifizierung auf der Basis von IT-Grundschutz* vollständig abgelöst.

Im Gegensatz zur ISO 27001 verfolgt der IT-Grundschutz den Bottom-Up-Ansatz und ist damit sehr techniklastig.

BSI IT Grundschutz

Grundschutzkatalog an Institutionen aller Größen und Arten

die eine […] zielführende Methode zum Aufbau und zur Umsetzung **der für sie angemessenen Informationssicherheit** benötigen

Eine besondere Bedeutung kommt dem BSI IT Grundschutz im Rahmen der **Zertifizierung nach ISO 27001** zu.

Da es sich bei ISO/IEC 27001 um eine internationale Norm handelt, besteht für die ISO-Zertifizierung zwar **keine Pflicht** zur Implementierung des BSI-Grundschutzes

Der IT-Grundschutz und die KRITIS-Verordnung werden **häufig verwechselt**, weil sie naturgemäß **ähnliche Themen** behandeln. Der Unterschied besteht darin, dass der Bund mit dem Grundschutz-Kompendium eine **pauschalisierte Vorgehensweise** für den **Schutz der Informationstechnik** von Unternehmen, Behörden und anderen Institutionen aller Größen geschaffen hat, deren Umsetzung jedoch **nicht verpflichtend** ist.

Alles was IT-Grundschutz nicht abbildet kann über die Cyberschutzversicherung abgebildet werden.

Links:

Passwortchecker: https://www.stmd.bayern.de/service/passwort-check/online-anwendung-passwort-check/

Hasso Plattner Institut(Ckeck auf Datenlecks der E-Mail-Adresse): https://sec.hpi.de/ilc/

Browsercheck: https://hpi-vdb.de/vulndb/sd_with_Sys_Browser/

BSI: https://www.bsi.bund.de/DE/Home/home_node.html

IT-Grundschutz: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium/checklisten_2021.html

IT-Grundschutz/Bausteine https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/IT-Grundschutz-Kompendium/IT-Grundschutz-Bausteine/Bausteine_Download_Edition_node.html

ISMS: https://www.tuev-nord.de/de/unternehmen/zertifizierung/iso-27001/#:~:text=Mit%20einer%20Zertifizierung%20nach%20ISO,Verbesserung%20eines%20ISMS%20gestellt%20werden.

Telekommunikationsnetze: Meldung des gewerblichen Betriebs von öffentlichen Telekommunikationsnetzen und/oder des gewerblichen Erbringens öffentlich zugänglicher Telekommunikationsdienste nach § 5 Telekommunikationsgesetz (TKG)

Meldeformular Bundesnetzagentur:
https://www.bundesnetzagentur.de/SharedDocs/Downloads/DE/Sachgebiete/Telekommunikation/Unternehmen_Institutionen/Anbieterpflichten/Meldepflicht/Meldeformular_pdf.pdf?__blob=publicationFile&v=8

- **elektronische Identifizierung und Vertrauensdienste (RFID, Barcode etc.)**

eIDAS-Verordnung

https://www.bsi.bund.de/DE/Themen/Oeffentliche-Verwaltung/eIDAS-Verordnung/eidas-verordnung_node.html

- **Anbieter digitaler Dienste**

(Online-Marktplätze, Online-Suchmaschinen, Cloud-Computing-Dienste)

BSI-Vorfall melden:

BSI-Meldung: https://www.bsi.bund.de/DE/IT-Sicherheitsvorfall/Kritische-Infrastrukturen-und-meldepflichtige-Unternehmen/Ich-muss-oder-moechte-einen-IT-Sicherheitsvorfall-melden/ich-muss-oder-moechte-einen-it-sicherheitsvorfall-melden_node.html

POLIZEI
Nordrhein-Westfalen
Kreis Lippe

Hilfe

- IT-Sicherheitsvorfall
- Cybercrime-Kompetenzzentrum LKA
- Onlineanzeige
- Polizeiwache vor Ort

POLIZEI
Nordrhein-Westfalen
Kreis Lippe

Die Zukunft von Cybercrime

- Firmenphilosopie bzw. Interpretation der Chefetage
- Deep Fake (Audio und Video)
- 5G Datenübertragung in Echtzeit

Von 2018…

Kreispolizeibehörde Lippe

Cybersicherheitsmanagement als Teil der Firmenkultur

CISO= Chief Information Security Officer

IT-Sicherheit ist Chefsache !!!!!!!

DEEP FAKE Obama 2018

Link: https://www.youtube.com/watch?v=cQ54GDm1eL0