



POLIZEI
Nordrhein-Westfalen
Landeskriminalamt

bürgerorientiert · professionell · rechtsstaatlich



Cybercrime - unterschätztes Risiko

Peter Vahrenhorst

Kriminalhauptkommissar

Landeskriminalamt NRW

SG 41.1 – Cybercrime-Kompetenzzentrum

Tel.: 0211 939 4114

Fax: 0211 939 19 4114

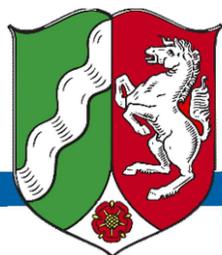
Peter.Vahrenhorst@polizei.nrw.de





POLIZEI
Nordrhein-Westfalen
Landeskriminalamt

Zahlen – Daten - Fakten



POLIZEI
Nordrhein-Westfalen
Landeskriminalamt

17.947.221 Einwohner

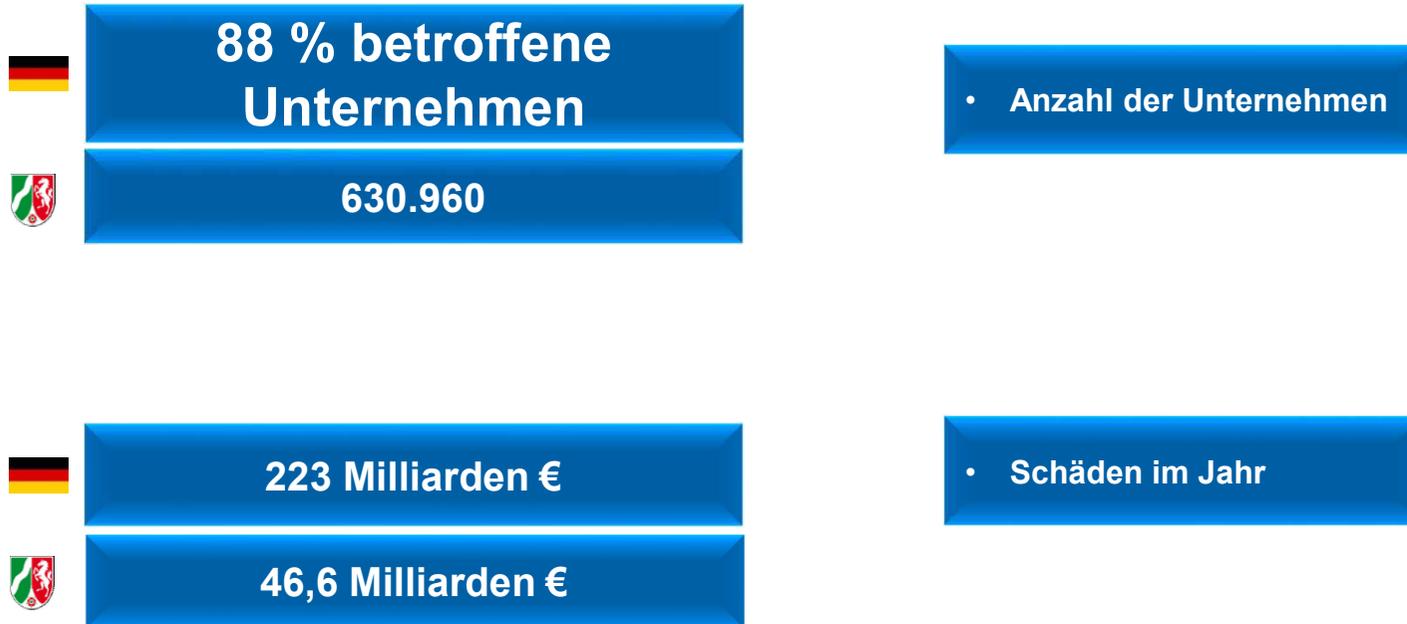
733 Mrd Euro BIP

Wirtschaftsstandort Nr. 1 in Deutschland

Wirtschaftsstandort Nr. 8 in Europa

717.000 KMU

Cybercrime als Gefahr für die Wirtschaft





POLIZEI
Nordrhein-Westfalen
Landeskriminalamt

Cyberangriffe haben bei
86% der Unternehmen
einen Schaden
verursacht

—

2019
waren es erst 70%

Neun Säulen-Modell: Cybercrime-as-a-Service





POLIZEI
Nordrhein-Westfalen
Landeskriminalamt

Fallbeispiel

Fall Beispiel „UKD“



POLIZEI
Nordrhein-Westfalen
Landeskriminalamt





POLIZEI
Nordrhein-Westfalen
Landeskriminalamt

Was ist zu tun?

Notfallmanagement



POLIZEI
Nordrhein-Westfalen
Landeskriminalamt

VERHALTEN BEI IT-NOTFÄLLEN



 **Ruhe bewahren & IT-Notfall melden**
Lieber einmal mehr als einmal zu wenig anrufen!

 **IT-Notfallrufnummer:**

 **Wer meldet?**

 **Welches IT-System ist betroffen?**

 **Wie haben Sie mit dem IT-System gearbeitet?**
Was haben Sie beobachtet?

 **Wann ist das Ereignis eingetreten?**

 **Wo befindet sich das betroffene IT-System?**
(Gebäude, Raum, Arbeitsplatz)

Verhaltenshinweise

Weitere Arbeit
am IT-System
einstellen

Beobachtungen
dokumentieren

Maßnahmen nur
nach Anweisung
einleiten

Herausgeber: Bundesamt für Sicherheit in der Informationstechnik

MASSNAHMEN-KATALOG ZUM NOTFALLMANAGEMENT



- Fokus IT-Notfälle -

Um eine ganzheitliche Cyber-Sicherheits-Strategie verfolgen zu können, sollten Sie ein Informations-Sicherheits-Management-System (ISMS) nach anerkannten Standards etablieren. Ein ISMS wird sinnvoll von einem Notfallmanagement/Business Continuity Management (BCM) ergänzt. Dieser Managementprozess obliegt den Notfallbeauftragten und beinhaltet u. a. die Erstellung folgender Produkte:

- einer Leitlinie zum Notfallmanagement,
- Entwicklung eines Notfallvorsorgekonzeptes sowie
- eines 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 vorschreitenden Digitalisierung stellen wollen und
- durch ein IT-Notfallmanagement die Cyber-Risiken ihres Unternehmens erheben 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 Vorabgespräche 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

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.

- | | |
|--|---|
| <input checked="" type="checkbox"/> Wurden erste Bewertungen des Vorfalles durchgeführt, um festzustellen, ob es sich um einen Cyber-Angriff oder lediglich um einen technischen Defekt handelt? | <input checked="" type="checkbox"/> Wurden Maßnahmen unternommen, um das gesamte Maß der Ausbreitung festzustellen? Wurden alle angegriffenen Systeme identifiziert? |
| <input checked="" type="checkbox"/> Haben Sie kontinuierlich Ihre Maßnahmen abgestimmt, dokumentiert und an alle relevanten Personen und Verantwortlichen kommuniziert? | <input checked="" type="checkbox"/> Wurden die beim Cyber-Angriff ausgetretenen Schwachstellen in Systemen oder (Geschäfts-) Prozessen durch relevante Maßnahmen adressiert und behoben? |
| <input checked="" type="checkbox"/> Wurden System-Protokolle, Log-Dateien, Notizen, Fotos von Bildschirmhalten, Datenträger und andere digitale Informationen forensisch gesichert? | <input checked="" type="checkbox"/> Wurden, nach Abstimmung, die Polizei oder relevante Behörden (Datenschutz, Meldepflichten, etc.) benachrichtigt? |
| <input checked="" type="checkbox"/> Haben Sie stets die besonders zeitkritischen und damit vorrangig zu schützenden Geschäftsprozesse im Fokus gehabt? | <input checked="" type="checkbox"/> Wurden die Zugangsberechtigungen und Authentifizierungsmethoden für betroffene (geschäftliche und ggf. private) Accounts überprüft (z.B. neue Passwörter, 2FA)? |
| <input checked="" type="checkbox"/> Wurden betroffene Systeme vom Netzwerk getrennt? Wurden Internetverbindungen zu den betroffenen Systemen getrennt? Wurden alle unautorisierten Zugriffe unterbunden? | <input checked="" type="checkbox"/> Wird das Netzwerk nach dem Vorfall weiter überwacht, um mögliche erneute Anomalien festzustellen? |
| <input checked="" type="checkbox"/> Wurden Backups getestet und vor möglichen weiteren Einwirkungen gesichert? | <input checked="" type="checkbox"/> Wurden die betroffenen Daten und Systeme wiederhergestellt oder neu aufgebaut? |

Das Dokument ist ein gemeinsames Produkt mehrerer Organisationen: Bundeskriminalamt, Charter of Trust, Deutscher Industrie- und Handelskammertag e.V., ivo – Verband der Internetwirtschaft e.V., Initiative Wirtschaftsinformatik, Nationale Initiative für Informations- und Internet-Sicherheit e.V., VDEIT – Bundesverband der IT-Anwender e.V., Allianz für Cyber-Sicherheit des Bundesamtes für Sicherheit in der Informationstechnik

Stand: September 2019



Backup-Strategie

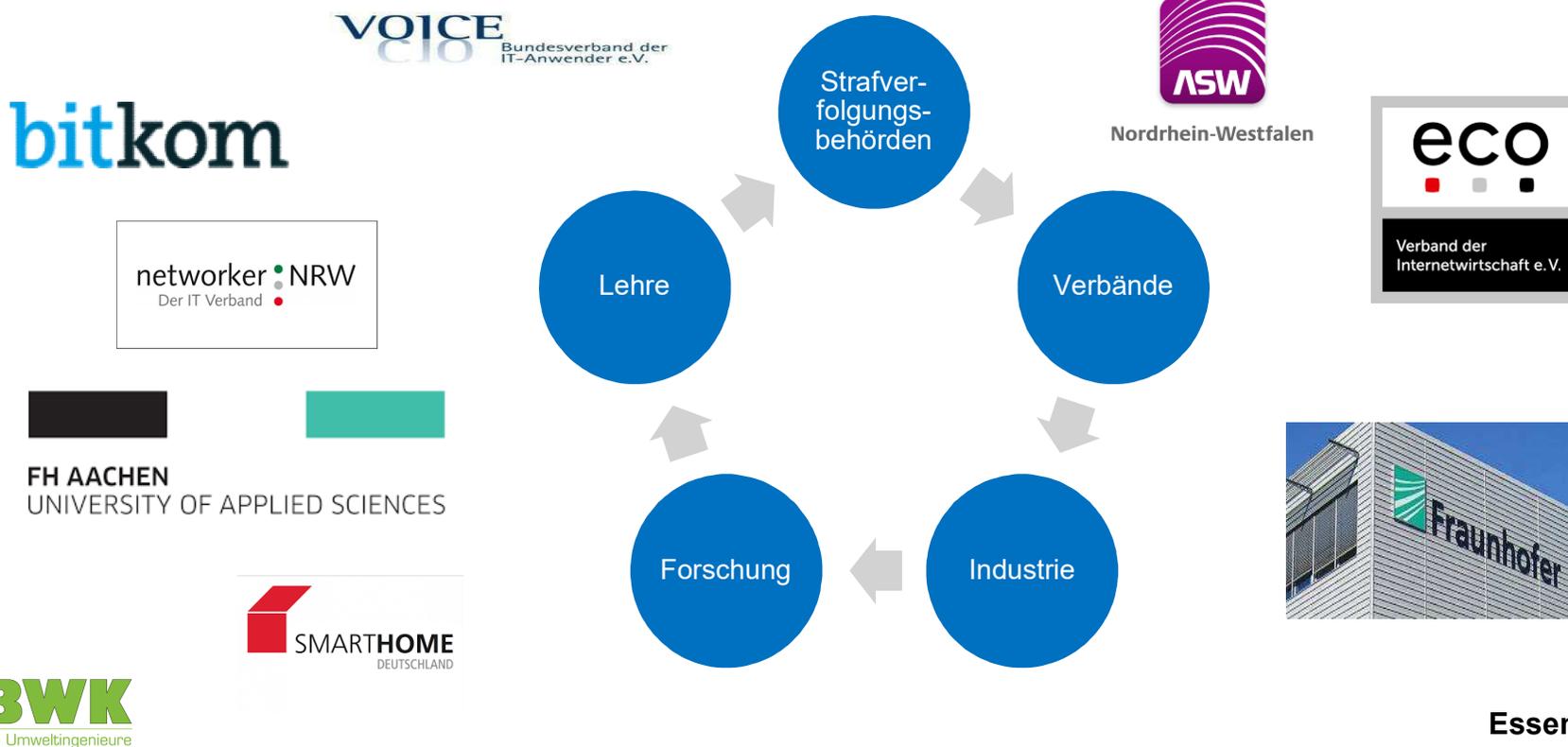
Datenintegrität



Kooperationen Gemeinsam gegen Cybercrime



POLIZEI
Nordrhein-Westfalen
Landeskriminalamt



Essen, 20.09.2022

Fragen?

Vielen Dank für Ihre Aufmerksamkeit.