

Vom Notfallhandbuch zum Notfallmanagement



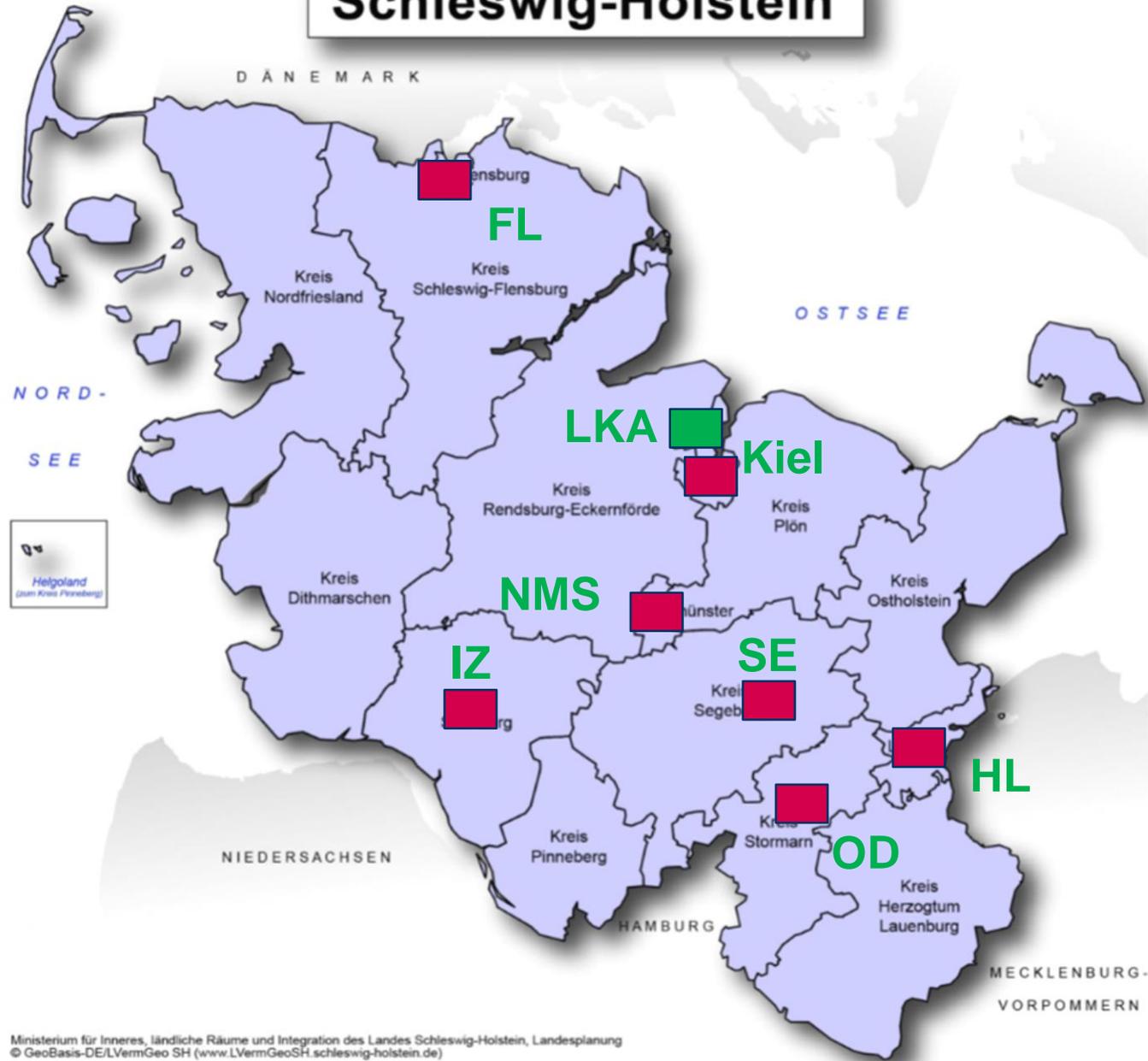
1. Forum Wirtschaftsschutz Schleswig-Holstein

Das Dezernat 23 im LKA S-H

Cybercrime und digitale Spuren



Schleswig-Holstein



**Ermittlungs-
dienststellen**

für

***herausragende
Cybercrime***



AUDIO: Stadtwerke Neumünster aktuell nicht erreichbar (1 Min)

Spionageversuch bei Stadtwerken Neumünster: Systeme bleiben abgeschaltet

Cybotage

Die Frage lautet nicht **OB**, sondern **WANN** Sie von einem Cyberangriff betroffen sein werden!

Stand: 28.08.2023 14:39 Uhr

Fast die gesamte Kommunikation der Stadtwerke Neumünster ist lahmgelegt - seitdem das Unternehmen einen Spionageversuch festgestellt hat. Das LKA ermittelt, die Analysephase läuft weiter.

1 Anfragen der

in gegebenen

Lar Die Kreisverwaltung bittet um Verständnis und Beachtung.



[Redacted]

PUBLISHED FILES

MORE →



[Redacted]

PUBLISHED FILES

Part#1 - 117736 files. Central Bank (FL) is headquartered in Tampa and is the 70th largest bank in the state of Florida. It is also the 2,663rd largest bank in the nation. It was established in 2007 e...

MORE →



[Redacted]

30 23H 0M 22 S

La storia dell'azienda Pietro Isnardi nasce dal profondo legame della famiglia alla propria terra, la Liguria, ricca di prodotti tipici d'eccellenza in cui la tradizione della coltura dell'ulivo ha oc...

MORE →



[Redacted]

PUBLISHED FILES

[Redacted] is a boutique litigation law firm with offices located in El Segundo, California, just minutes from Los Angeles International Airport. The Firm specializes in business and comm...

MORE →



[Redacted]

PUBLISHED FILES

We have been serving the stone industry for over 50 years. The experience gained, the passion for natural stone - unique and unrepeatable - the highly specialized staff and cutting-edge machinery allo...

MORE →



[Redacted]

PUBLISHED FILES

For us AMBAUers, this means always looking at the human side of everything, making an effort to remain and act humanely... even when there are major problems in society.

MORE →



[Redacted]

PUBLISHED FILES

The best of wood for the garden: This is what the [Redacted] brand stands for, based in Daldorf in northern Germany. Our experience with wood dates back to 1948 - since 1984 we have been concentrating on...



[Redacted]

PUBLISHED FILES

Saint-Cloud, chef-lieu de canton du département des Hauts-de-Seine (92), se situe à 5 kilomètres à l'ouest de Paris

MORE →



[Redacted]

PUBLISHED FILES

The Ministry of Justice of France is a body of the French government, which is responsible for: supervision of the judiciary, its maintenance and administration; participation as Vice President of the...

s. Wir sind
struktur
eßlich auf
eten der
n.
rt und
BDSG)

Problemlage KMU

„Die Bedrohung im Cyberraum ist so hoch wie nie.“
2021 sind 66 Zero-Day-Schwachstellen bekannt geworden



In Deutschland existieren nach EU-Klassifikation etwa **2,6 Millionen Unternehmen**, die dem Bereich KMU zuzurechnen sind, das sind 99,4 Prozent aller Unternehmen in Deutschland.



„Gerade die Kleinst- (weniger als zehn Mitarbeitende) und die kleinen (weniger als 50 Mitarbeitende) Unternehmen verfügen oftmals nicht über das erforderliche Personal, das sich um Betrieb und Absicherung der Informationstechnik des Unternehmens kümmert.“



„Dies alles führt dazu, dass einige KMU zum einen Opfer Cyber-Krimineller werden und zum anderen auf einen Vorfall nicht angemessen reagieren können. (...) Im Ereignisfall wissen KMU oftmals nicht, an wen sie sich wenden können, um fachlich versierte Hilfe zu erhalten.“

Quellen: BSI Lagebericht IT-Sicherheit 2022 und Bericht der European Union Agency for Cybersecurity 2022



Besteht überhaupt Handlungsbedarf?

Bei kleineren und mittleren Unternehmen (KMU) ist es hierzulande um die IT-Security nach wie vor schlecht bestellt. Schon bei Standardschutzmaßnahmen sind die Defizite bei ihnen groß, geht es aus dem "Praxisreport Mittelstand" 2021/22 hervor, den der Verein "Deutschland sicher im Netz" (DsiN) am Dienstag vorgestellt hat. Demnach verfügen 64 Prozent der KMU über keine Maßnahmen der Angriffserkennung, mehr als ein Drittel verzichtet auf IT-Notfallpläne (34 Prozent).

Bewusstsein für Sicherheitsrisiken da, aber das Handeln fehlt

Der vom Bundeswirtschaftsministerium unterstützte Bericht beruht auf einer repräsentativen Erhebung von 1339 abgeschlossenen Umfragen des DsiN-Sicherheitschecks im Zeitraum von Mai 2020 bis Januar 2022. 43 Prozent der Mittelständler sind demnach nachlässig im Umgang mit Software- und Sicherheitsupdates. Von Schutzvorkehrungen in der E-Mailkommunikation sieht die Hälfte der KMU ab, verschlüsselt also nicht. Ein Viertel der Firmen verzichtet vollständig darauf, das IT-Sicherheitswissen bei Mitarbeitern zu fördern.



Management von Cyber-Risiken

Ein Handbuch für die Unternehmensleitung



PRINZIP 1

Cyber-Sicherheit nicht nur als IT-Thema, sondern als Baustein des unternehmensweiten Risikomanagements verstehen

Die Unternehmensleitung muss die Cyber-Sicherheit nicht nur als IT-Risiko, sondern als strategisches Unternehmensrisiko verstehen und angehen.



PRINZIP 2

Rechtliche Auswirkungen von Cyber-Risiken verstehen

Die Unternehmensleitung sollte die rechtlichen Auswirkungen von Cyber-Risiken in Bezug auf die individuellen Anforderungen ihres Unternehmens verstehen.



PRINZIP 3

Zugang zu Cyber-Sicherheitsexpertise sowie regelmäßigen Austausch sicherstellen

Die Unternehmensleitung sollte einen angemessenen Zugang zu Cyber-Sicherheits-Expertise fordern. Diskussionen über Cyber-Risikomanagement sollten regelmäßig und in angemessenem Umfang auf die Tagesordnung gesetzt werden.



PRINZIP 4

Umsetzung geeigneter Rahmenbedingungen sowie Ressourcen für das Cyber-Risikomanagement sicherstellen

Die Unternehmensleitung sollte die Erwartung formulieren, dass das Management einen unternehmensweiten Rahmen für das Cyber-Risikomanagement mit adäquater Personalausstattung und angemessenem Budget schafft.



PRINZIP 5

Risikoanalyse erstellen sowie Definition von Risikobereitschaft in Abhängigkeit von Geschäftszielen und -strategien formulieren

Im Austausch zwischen Unternehmensleitung und Management über Cyber-Sicherheit sollte die Identifizierung und Quantifizierung der finanziellen Kosten in Bezug auf Cyber-Risiken diskutiert werden. Insbesondere sollte die Frage besprochen werden, welche Risiken akzeptiert, gemindert oder übertragen werden sollen, z. B. durch eine Versicherung, sowie spezifische Pläne, die mit jedem Ansatz verbunden sind.



PRINZIP 6

Unternehmensweite Zusammenarbeit und den Austausch von Best Practice fördern

Die Unternehmensleitung sollte die Zusammenarbeit innerhalb ihrer Branche und mit öffentlichen und privaten Akteuren fördern, um sicherzustellen, dass jede Institution die Resilienz Aller unterstützt.

- ✓ Verantwortlichkeiten für den Fall der Fälle festlegen
- ✓ Bestimmung eines organisationsübergreifenden Cyber-Risikomanagement-Teams
- ✓ Entwicklung einer Strategie für das Management von Cyber-Risiken sowie eine Kommunikationsstrategie
- ✓ Vorhalten eines ausreichenden Cyber-Risiko-Budgets

Und im Fall der Fälle? (I)

Fehlerkultur

Notfallplan

Erstattung einer
Strafanzeige

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

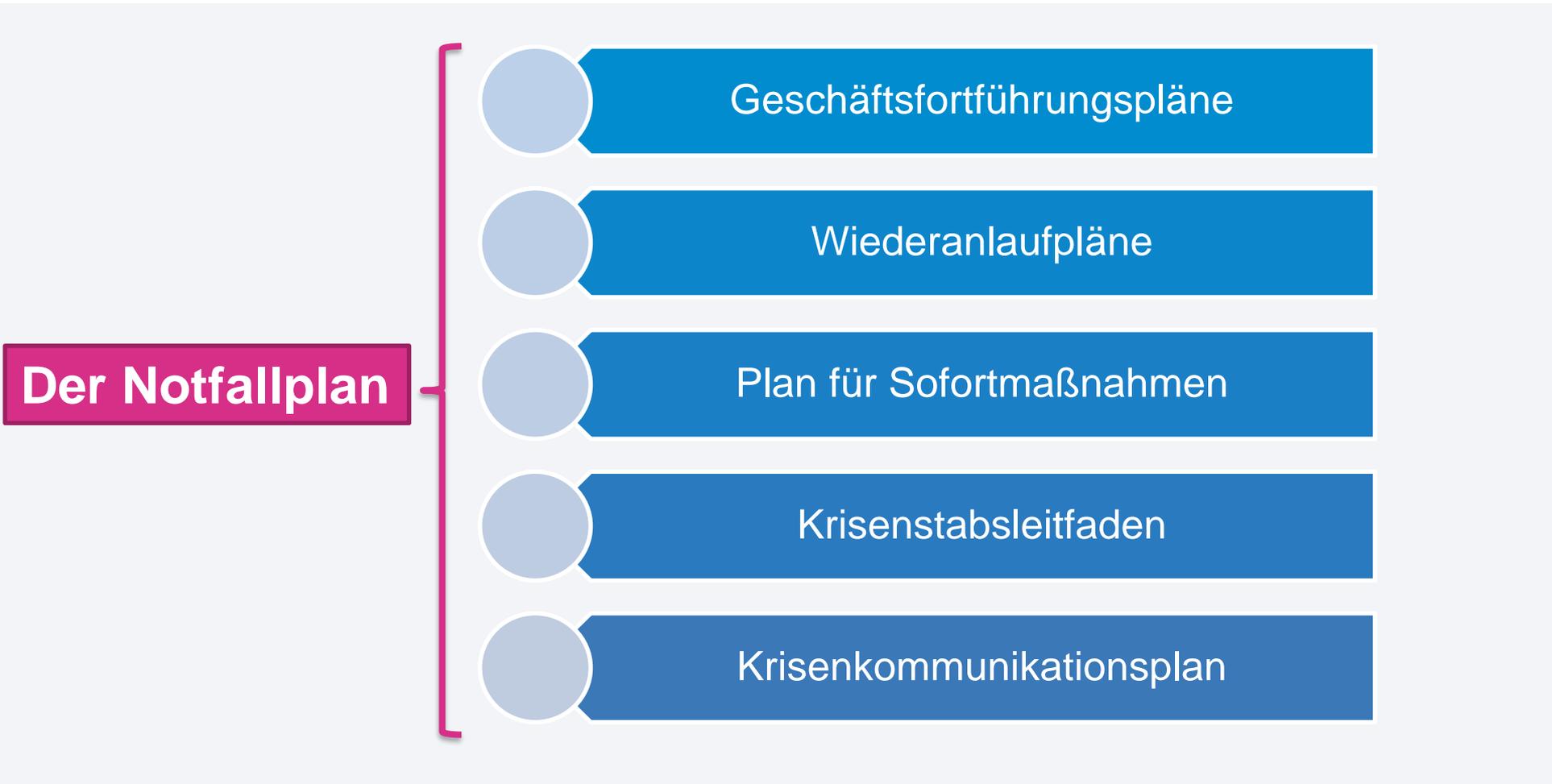
Weitere Arbeit
am IT-System
einstellen

Beobachtungen
dokumentieren

Maßnahmen nur
nach Anweisung
einleiten

Herausgeber: Bundesamt für Sicherheit in der Informationstechnik

Und im Fall der Fälle? (II)



Und im Fall der Fälle? (III)



Und im Fall der Fälle? (IV)

Im Falle eines Cybercrime-Vorfalles ist entschlossenes und schnelles Handeln erforderlich!

Denn Insbesondere in diesem Deliktsfeld sind Beweismittel nur in engen Zeitfenstern zuverlässig zu sichern und zu verwerten. Ebenso ist ein zeitnahes Eingreifen geboten, um größere Schäden an Hard-, Software und kostbaren Daten zu vermeiden. Auch sind Ausmaß und Folgen eines digitalen Angriffs anfänglich oftmals kaum abschätzbar.

Ihr Unternehmen/Ihre Behörde ist in Schleswig-Holstein ansässig? **0431 160-42727**

Rufen Sie die **Hotline 0431 160-42727** an oder übersenden uns Ihr Anliegen über das **unten stehende Kontaktformular**.

Falls Sie uns nicht erreichen können:

- Wenden Sie sich in dringenden Fällen an den **Notruf 110**.
- Bei einem aktuellen oder andauernden Verschlüsselungsangriff einzelner oder gesamter IT-Strukturen, wenden Sie sich an das Lagezentrum der Landespolei Schleswig-Holstein unter der Rufnummer 0431 160-61111.



Folgen eines IT-Sicherheitsvorfalls und einer Strafanzeige

Sicherheitsvorfall

- betroffene Unternehmen schalten in den "Überlebensmodus"
- Versuch, mit möglichst wenig Aufwand wieder arbeitsfähig zu werden



VS.

nach der Strafanzeige

- "gefühl": keine Hilfe durch die Polizei
- Wir benötigen u. a.:
 - Hinweise zur "Initialinfektion"
 - Art der Malware
 - Logfiles
 - Sicherungen wichtiger Systemserver
 - Eventuelle Kommunikation mit den Tätern
 - Rahmendaten zum Unternehmen
 - Schadensausmaß

Polizei:

- Erfahrung
- Beratung in Hinblick auf die/den Täter
- Handlungssicherheit
- → sehr wohl Hilfe!

Wenn wir nicht **ZUSAMMEN** diesen **Aufwand** betreiben, werden wir die **Täter NIEMALS** ermitteln!



Und im Fall der Fälle? (V)

Serviceleistungen der Polizei:

- Anzeigenaufnahme
- Beratung
- Ggf. Vermittlung von Ansprechpartnern für IT-Dienstleister
- Vertrauensvolle Zusammenarbeit



Was wir nicht machen



Hardware mitnehmen, Betrieb lahmlegen



„schnüffeln“, aktiv nach möglichen
Verstößen oder Straftaten hin suchen,
bzw. Asservate untersuchen



Störung der Abläufe



Einschränkung der Handlungsfreiheit

Wir haben verstanden: es brennt in der Firma

Weitergehende Informationen



Schleswig-Holstein
Landespolizei

Die stets aktuellen Kontaktdaten der Zentralen Ansprechstellen Cybercrime erhalten Sie unter www.polizei.de:



Weitergehende Informationen und Handlungsempfehlungen für Unternehmen finden Sie hier:



Hier können Sie sich informieren!



 Bundeskriminalamt 

Es hat Sie erwischt!

CYBER- ANTACKE AUF IHR UNTERNEHMEN,
IHRE BEHÖRDE ODER INSTITUTION

Sie haben Vorbehalte, uns einzuschalten?
Das haben wir verstanden!
Lassen Sie uns reden.



Ihre Firma

Was bringt es mir, die Polizei zu kontaktieren?
Die finden den oder die Täter doch sowieso nicht.

Täterermittlungen sind lediglich ein Strang.
Wir werden nicht jeden Hacker finden können. Aber wir können deren IT-Infrastruktur stören oder herunternehmen oder an ihr Geld kommen.

 **Strafverfolgung**

Wenn ich die Polizei verständige, nimmt sie große Teile meiner Hardware mit und bringt sie nicht oder nicht zeitnah zurück.

Wir müssen nicht in jedem Fall bei Ihnen im Unternehmen aktiv werden. In vielen Fällen können Sie uns relevante Daten einfach aushändigen. Nur in Einzelfällen ist eine Datensicherung vor Ort durch die Polizei erforderlich, die wir natürlich mit Ihnen abstimmen.

Polizei und Staatsanwaltschaft ermitteln dann eher gegen mich, wenn sie etwas Belastendes gefunden haben. Dabei bin ich/sind wir das Opfer der Attacke und haben andere Sorgen.

Wir sind auf den Sachverhalt fokussiert, bei dem Sie geschädigt sind. Im Übrigen geben Sie uns die Daten, wir suchen nicht danach in Ihren Systemen.

Wenn ich heute mit der Polizei oder Staatsanwaltschaft spreche, steht morgen alles in der Presse!

Das Gegenteil ist der Fall, gerade in der frühen Phase der Ermittlungen werden generell keine proaktiven Presseauskünfte erteilt. Auch im weiteren Verlauf stimmen wir die Pressearbeit mit Ihnen ab.

Wenn ich Polizei und Staatsanwaltschaft einbinde, darf ich doch am Ende gar nichts mehr entscheiden, also etwa ob ich Erpressungsgeld zahle oder mit den Tätern kommuniziere.

Sie entscheiden - wir beraten. Sie können von unserer Erfahrung in solchen Angriffssituationen profitieren.



Was braucht die Strafverfolgung eigentlich?

-  Die Daten zu einem Angriff liegen bei Ihnen. In den Daten liegen die Spuren zu den Tätern und ihrer Infrastruktur.
- Wir möchten **schnellstmöglich** mit diesen Daten arbeiten.
- Wir benötigen von Ihnen:** Malwaresamples, (IP-Adressen aus) Logfiles, E-Mailadressen, von denen mit Ihnen kommuniziert wurde, jede Information zur Täterkommunikation, Hinweise auf Leak-Pages...
-  Wir wissen, dass es bei Ihnen **brennt**. Darauf werden wir Rücksicht nehmen. Die Rettung Ihres Unternehmens steht im Fokus Ihres Tuns.
- Daten sind für uns auch von extrem großem Wert, wenn Sie im Eifer des Gefechts **nicht forensisch** gesichert wurden.
- Unsere Empfehlung: Binden Sie die Polizei frühzeitig ein!**
- Lassen Sie Ihre Techniker oder beauftragte IT Security Unternehmen mit unseren Technikern sprechen und sich von uns beraten.
- Wir finden einen Weg, Sie möglichst wenig zu belasten und so schnell wie möglich an notwendige Spuren zu kommen.

Wer hilft mir weiter?

Die **Zentralen Ansprechstellen Cybercrime (ZAC)** der Polizeien des Bundes und der Länder stehen **Unternehmen und öffentlichen Einrichtungen** als kompetente und vertrauensvolle Partner zur Verfügung

- für Informationen und Beratung zur Vermeidung von Cybercrime-Angriffen (Prävention)
- für richtiges Verhalten bei Cybercrime-Angriffen gegen Ihr Unternehmen (Intervention, Strafverfolgung).

Das Bundeskriminalamt ist unmittelbar zuständig für die Strafverfolgung bei Cyberangriffen auf **Kritische Infrastrukturen** (sog. KRITIS-Unternehmen) sowie auf **Behörden und Einrichtungen des Bundes**. Ansprechpartner ist in diesen Fällen die **ZAC BKA** sowie die 24/7 erreichbare **Eltsatzbereitschaft Cybercrime**.

In **allen anderen Fällen** sind die **Cybercrime-Dienststellen der Landespolizei** zuständig. Die örtlich zuständige Dienststelle sowie Informationen und Beratung zum Phänomenbereich Cybercrime erhalten Sie über die **ZAC** der Landeskriminalämter (**ZAC LKÄ**).

Bei vielen ZACs findet außerhalb der Bürozeiten eine Weiterleitung an einen Bereitschaftsdienst statt. In **akuten Notfällen**, wenn mit den angegebenen Nummern kein Kontakt hergestellt werden kann, ist auch die Wahl des Notrufes denkbar.

ZAC BUNDESKRIMINALAMT
Referat CC12-ZAC
65173 Wiesbaden
Tel. (reg.): 0611/55-15037
Internet: www.bka.de

ZAC LKÄ



WEBSEITE





Es hat Sie erwischt!
CYBER- ANGRIFE AUF IHR UNTERNEHMEN,
IHRE BEHÖRDE ODER INSTITUTION

Sie haben Vorbehalte, uns einzuschalten?
Das haben wir verstanden!
Lassen Sie uns reden.



Die Daten zu einem Angriff liegen bei Ihnen. In den Daten liegen die Spuren zu den Tätern und ihrer Infrastruktur.

Wir möchten **schnellstmöglich** mit diesen Daten arbeiten.



Wir benötigen von Ihnen:
Malwaresamples, (IP-Adressen aus) Logfiles, E-Mailadressen,
von denen mit Ihnen kommuniziert wurde, jede Information zur
Täterkommunikation, Hinweise auf Leak-Pages...



Wir wissen, dass es bei Ihnen **brennt**. Die Rettung Ihres Unternehmens ist unsere oberste Priorität.

Daten sind für uns auch von extrem großem Wert, wenn Sie im Eifer des Gefechts **nicht forensisch** gesichert wurden.

Unsere Empfehlung: Binden Sie Ihre Techniker oder beauftragte IT Security Unternehmen mit unseren Technikern sprechen und sich von uns beraten.

Lassen Sie Ihre Techniker oder beauftragte IT Security Unternehmen mit unseren Technikern sprechen und sich von uns beraten.

Wir finden einen Weg, Sie möglichst wenig zu belasten und so schnell wie möglich an notwendige Spuren zu kommen.



Die Daten zu einem Angriff liegen bei Ihnen. In den Daten liegen die Spuren zu den Tätern und ihrer Infrastruktur.

Wir möchten **schnellstmöglich** mit diesen Daten arbeiten.



Wir benötigen von Ihnen:
Malwaresamples, (IP-Adressen aus) Logfiles, E-Mailadressen,
von denen mit Ihnen kommuniziert wurde, jede Information zur
Täterkommunikation, Hinweise auf Leak-Pages...



Wir wissen, dass es bei Ihnen **brennt**. Darauf werden wir Rücksicht nehmen. Die Rettung Ihres Unternehmens steht im Fokus Ihres Tuns.

Unsere Empfehlung: Binden Sie die Polizei frühzeitig ein!

Lassen Sie Ihre Techniker oder beauftragte IT Security Unternehmen mit unseren Technikern sprechen und sich von uns beraten.

Wir finden einen Weg, Sie möglichst wenig zu belasten und so schnell wie möglich an notwendige Spuren zu kommen.

Wer hilft mir weiter?

Zentralen Ansprechstellen für Cybercrime (ZAC) der Polizeien des Bundes und der Länder stehen Unternehmen und öffentlichen Einrichtungen als kompetente und zuverlässige Partner zur Verfügung

Für Informationen und Beratung zur Vermeidung von Cybercrime-Angriffen (Prävention) für richtiges Verhalten bei Cybercrime-Angriffen gegen Ihr Unternehmen (Intervention, Strafverfolgung).

Bundeskriminalamt ist unmittelbar zuständig für Cybercrime-Strukturen. Wie auf Behörden-Einrichtungen des Bundes. Ansprechpartner ist in diesen Fällen die AC BKA sowie die 24/7 erreichbare Einsatzbereitschaft Cybercrime.

In anderen Fällen sind die Cybercrime-Dienststellen der Landespolizeibehörden zuständig. Die zuständige Dienststelle sowie Informationen und Beratung zum themenbereich Cybercrime erhalten Sie über die ZAC der Landespolizei (ZAC LKA).

Bei vielen ZACs findet außerhalb der Bürozeiten eine Weiterleitung an einen Bereitschaftsdienst statt. In akuten Notfällen, wenn mit den angegebenen Nummern kein Kontakt hergestellt werden kann, ist auch die Wahl des Notrufes denkbar.

ZAC BUNDESKRIMINALAMT
Referat CCI2-ZAC
65173 Wiesbaden
Tel. (reg.): 0611/55-15037
Internet: www.bka.de

cht
Tuns.
Eifer

sh-



WEBSITE

Ein Hinweis zum Schluss...

Meldepflicht bei der Aufsichtsbehörde nach Art. 33 DSGVO

*(1) Im Falle einer Verletzung des Schutzes personenbezogener Daten meldet der Verantwortliche **unverzüglich und möglichst binnen 72 Stunden**, nachdem ihm die Verletzung bekannt wurde, diese der gemäß Artikel 55 zuständigen Aufsichtsbehörde, es sei denn, dass die Verletzung des Schutzes personenbezogener Daten voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt. Erfolgt die Meldung an die Aufsichtsbehörde nicht binnen 72 Stunden, so ist ihr eine Begründung für die Verzögerung beizufügen.*

Beachte Art. 34: Unverzügliche Benachrichtigung der betroffenen Person(en) bei hohem Risiko für die persönlichen Rechte und Freiheiten (z.B. Identitätsdiebstahl, Reputationsschädigung)

www.datenschutzzentrum.de/uploads/formular/Meldung-Datenpanne.odt (Formular)



**Vielen Dank für Ihre
Aufmerksamkeit!**

Fragen?



Lars Oeffner
Leiter Dezernat 23

Jannika Grade
Zentrale Ansprechstelle
Cybercrime (ZAC)

Cybercrime-Hotline: **0431-160-42727**

E-Mail: cybercrime@polizei.landsh.de