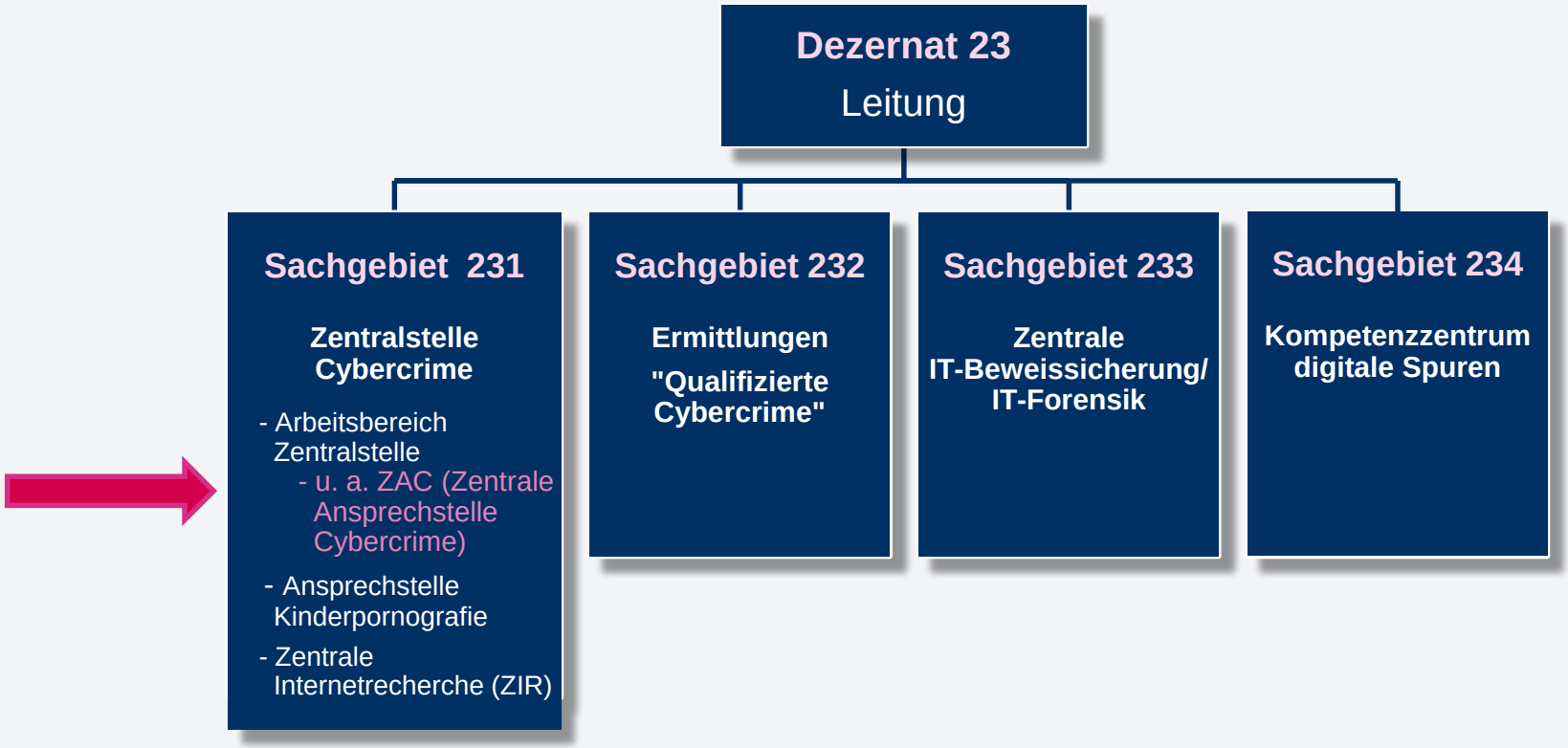
Vom Notfallhandbuch zum Notfallmanagement

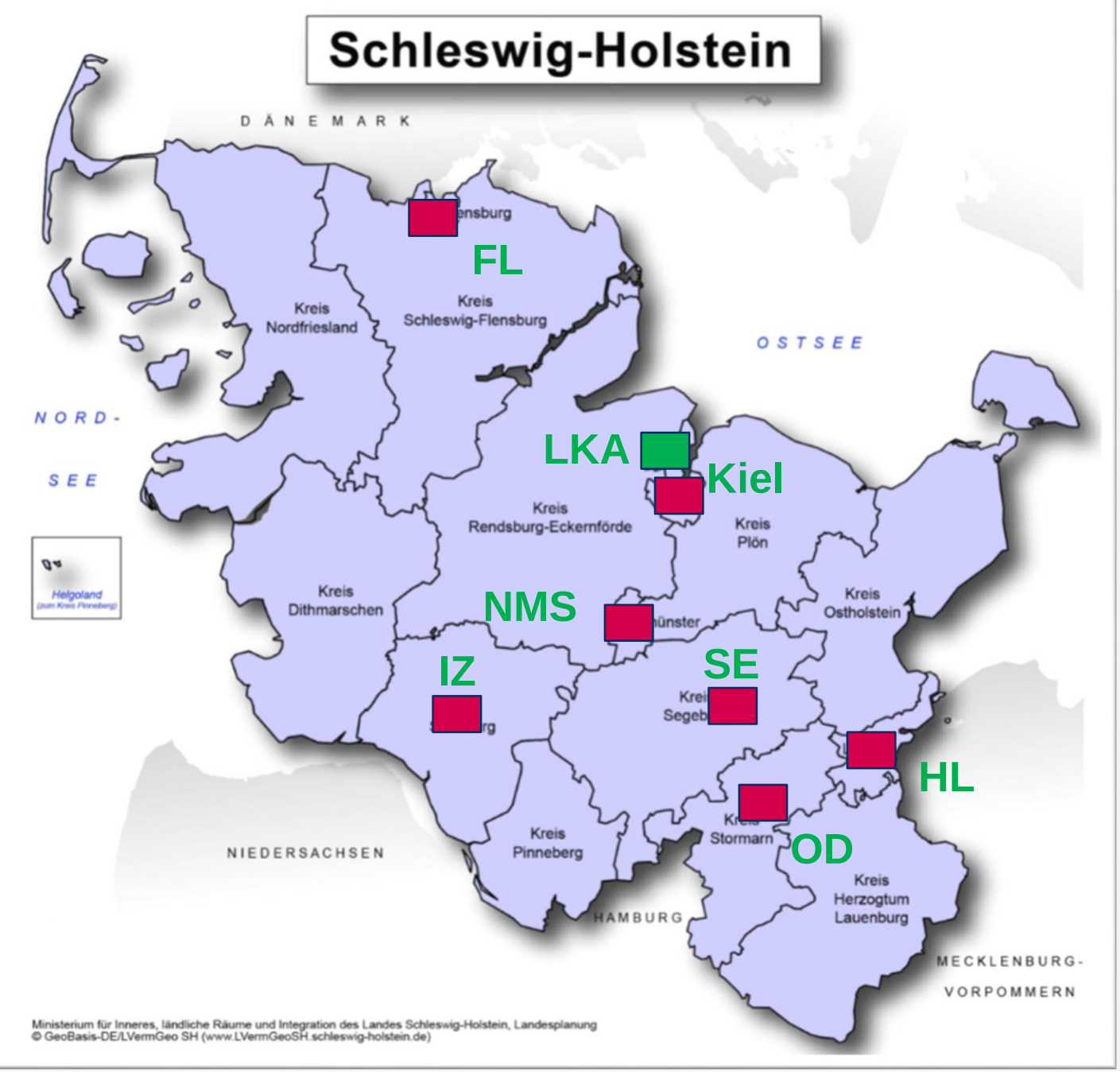
Schleswig-Holstein
Landespolizei

1. Forum Wirtschaftsschutz Schleswig-Holstein

Das Dezernat 23 im LKA S-H
Cybercrime und digitale Spuren

Schleswig-Holstein
Landespolizei





SH Schleswig-Holstein
Landespolizei

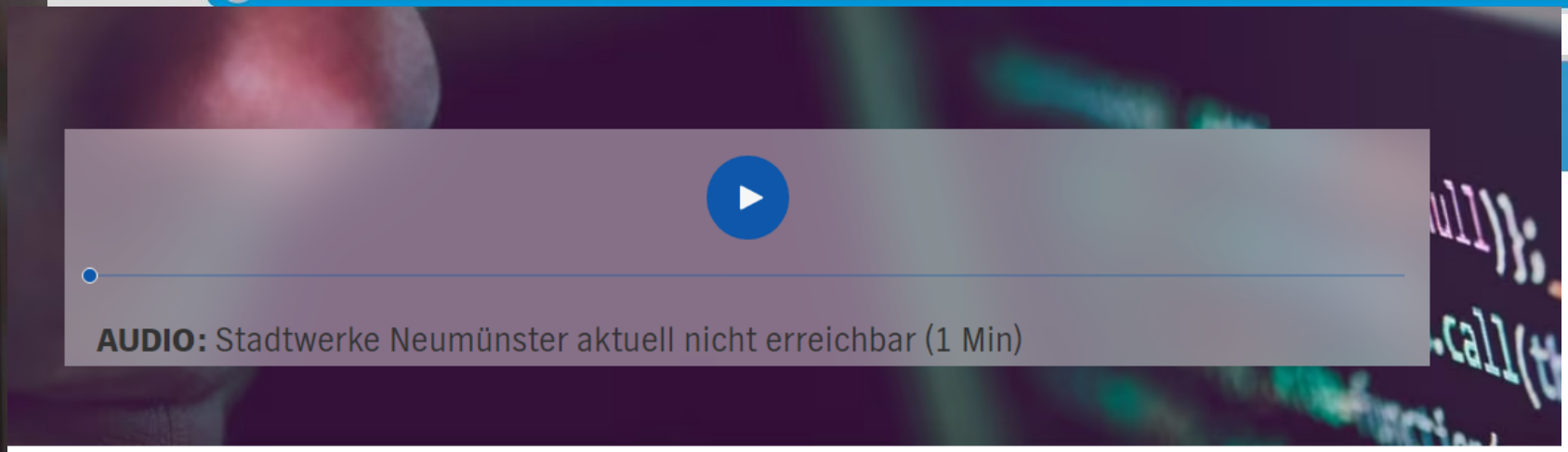
Ermittlungs-dienststellen

für

herausragende Cybercrime

NETZWELT

SWR AKTUELL



Spionageversuch bei Stadtwerken Neumünster: Systeme bleiben abgeschaltet

Cybotage

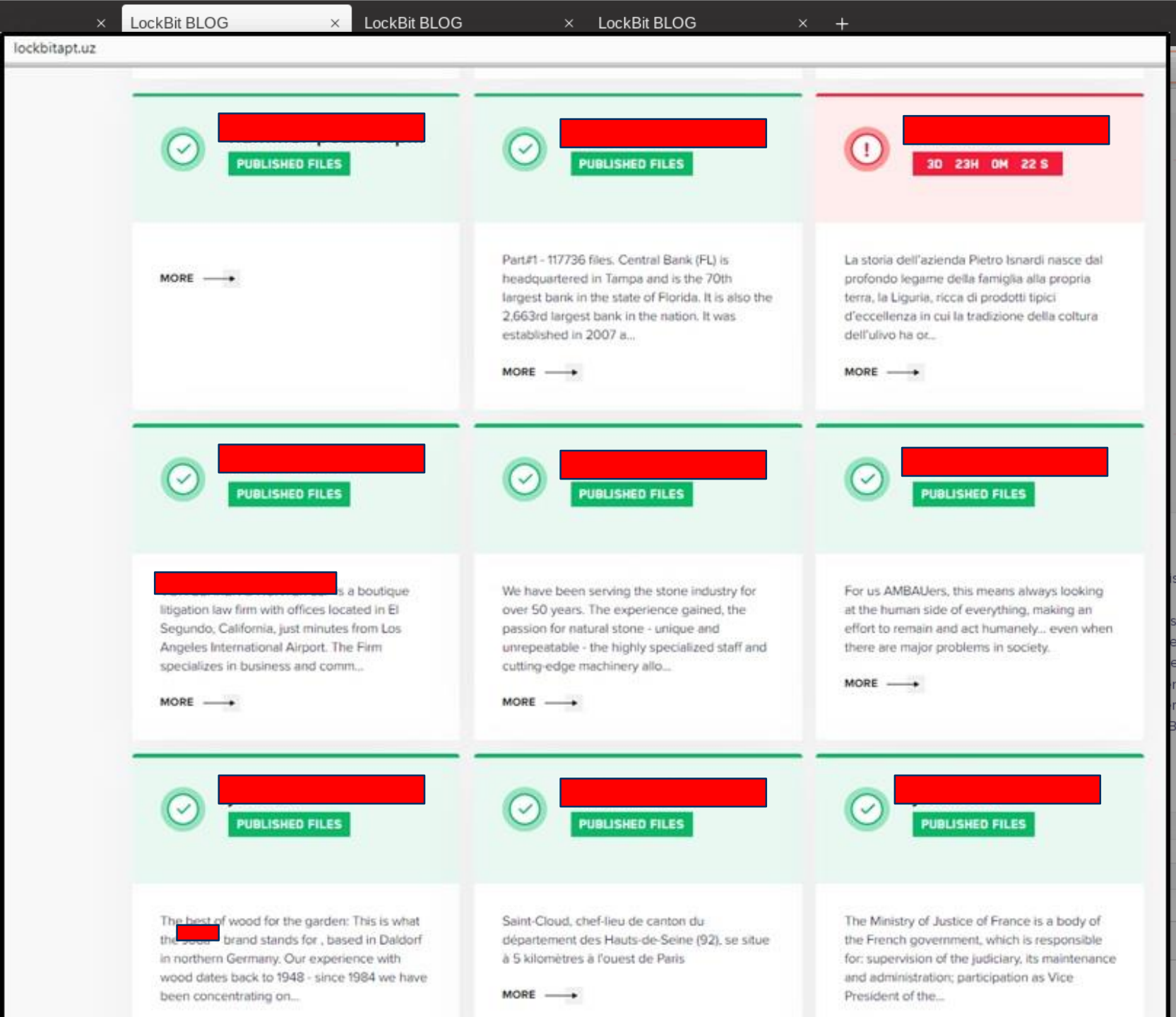
Die Frage lautet nicht **OB**, sondern **WANN** Sie von einem Cyberangriff betroffen sein werden!

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.

Die Kreisverwaltung bittet um Verständnis und Beachtung.

Schleswig-Holstein. Der echte Norden.


LockBit BLOG
LockBit BLOG
LockBit BLOG
lockbitapt.uz
[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 a...
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 or...
MORE
[redacted]
PUBLISHED FILES
[redacted] s 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...

Problemlage KMU

Schleswig-Holstein
Landespolizei

„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?

Schleswig-Holstein
Landespolizei

Bei kleineren und mittleren Unterne[illegible]en (KMU) ist es hierzulande um die IT-Security nach wie vor schlecht beste[illegible] Schon bei Standardschutzmaßnahmen sind die Defizite bei ihnen groß, geht[illegible]s dem "Praxisreport Mittelstand" 2021/22 hervor, den der Verein "Deutschland[illegible]ner 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.

Schleswig-Holstein
Landespolizei

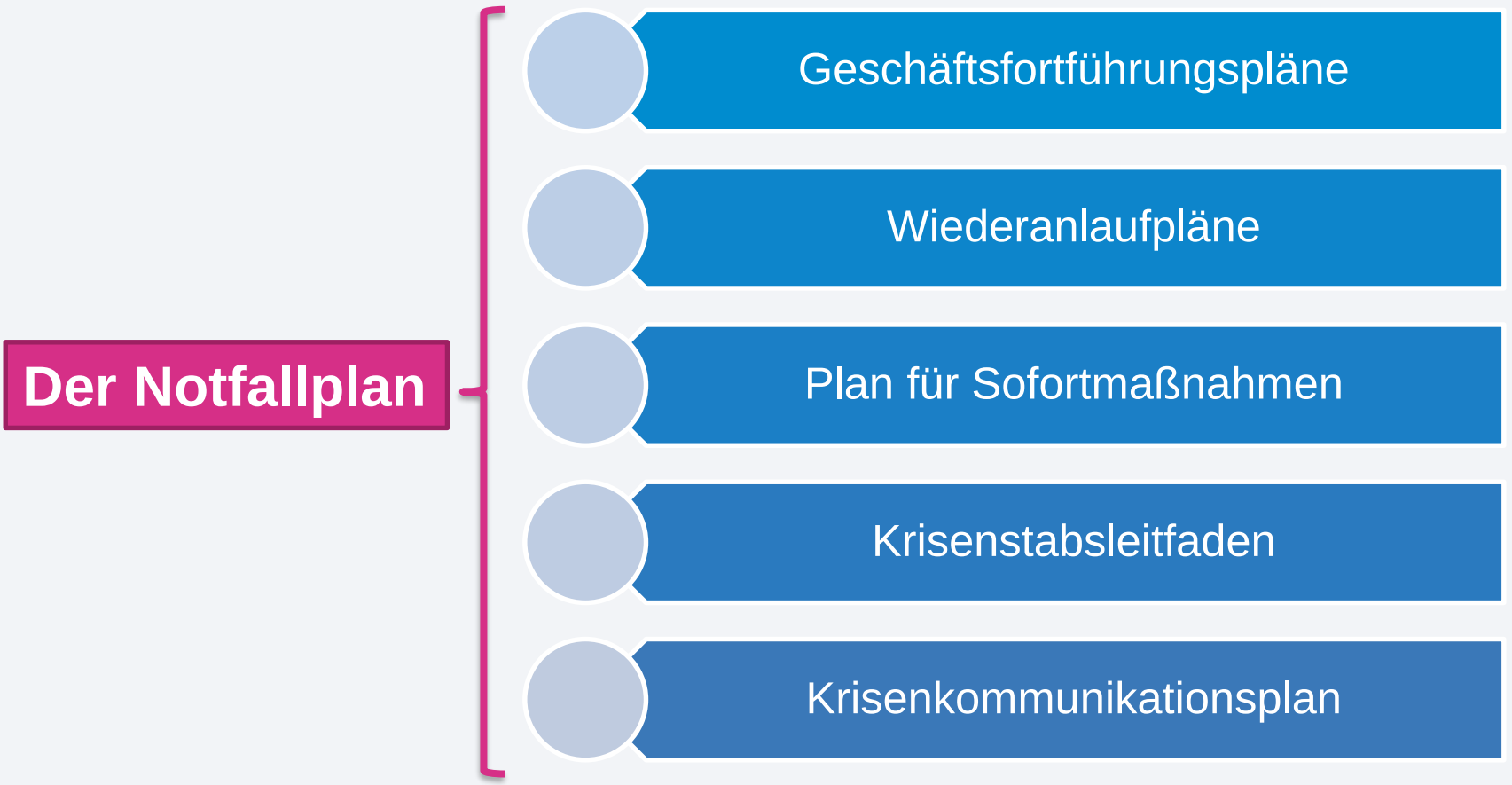
- ✓ Verantwortlichkeiten für den Fall der Fälle festlegen
- ✓ Bestimmung eines organisationsübergreifenden Cyber-Risikomanagement-Teams
- ✓ Entwicklung einer Strategie für das Management von Cyber-Risiken sowie eine Kommunikationsstrategie
- ✓ Vorhalten eines ausreichenden Cyber-Risiko-Budgets

Und im Fall der Fälle? (I)

- Fehlerkultur
- Notfallplan
- Erstattung einer Strafanzeige

Und im Fall der Fälle? (II)

Schleswig-Holstein
Landespolizei



Und im Fall der Fälle? (III)

Schleswig-Holstein
Landespolizei

Und im Fall der Fälle? (IV)

Schleswig-Holstein
Landespolizei

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 Landespolizei Schleswig-Holstein unter der Rufnummer 0431 160-61111.

Folgen eines IT-Sicherheitsvorfalls und einer Strafanzeige

Schleswig-Holstein
Landespolizei

Sicherheitsvorfall

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

vs.

nach der Strafanzeige

- "gefühlt": 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)

Schleswig-Holstein
Landespolizei

Serviceleistungen der Polizei:

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

Was wir nicht machen

Schleswig-Holstein
Landespolizei

- 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:

Schleswig-Holstein
Landespolizei

Hier können Sie sich informieren!

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 **Einsatzbereitschaft Cybercrime**.

In **allen anderen Fällen** sind die **Cybercrime-Dienststellen der Landespolizeibehörden** 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

Schleswig-Holstein
Landespolizei

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 cht
nehmen. Die Rettung Ihres U Tuns.

Daten sind für uns auch von e Eifer
des Gefechts **nicht forensisch**

Unsere Empfehlung: Binden

Lassen Sie Ihre Techniker od eh-
men 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.

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.

Ein Hinweis zum Schluss…

Schleswig-Holstein
Landespolizei

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

SH Schleswig-Holstein
Landespolizei