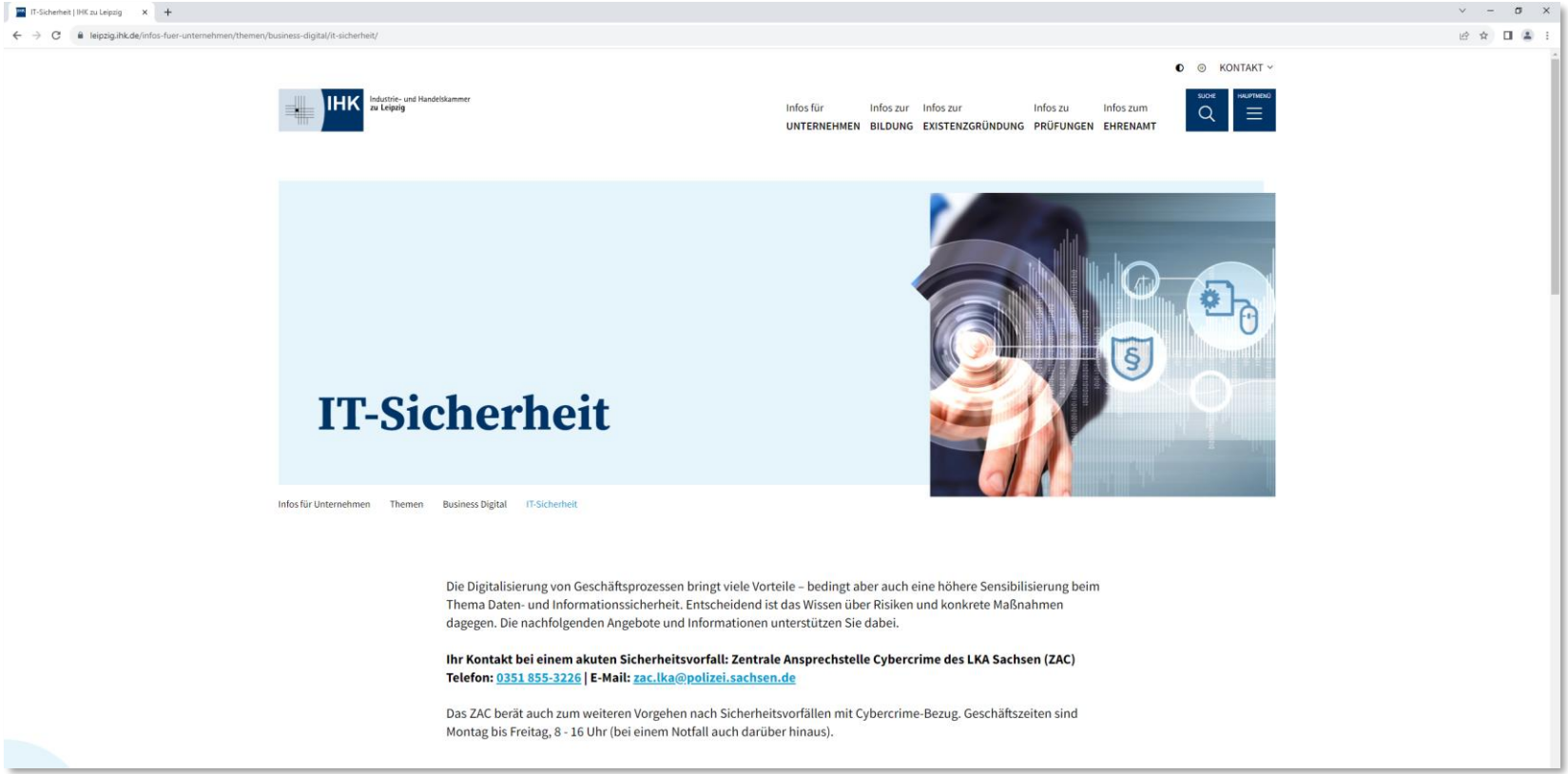
Informationssicherheit in Unternehmen

Übersicht Unterstützungsmöglichkeiten

IHK

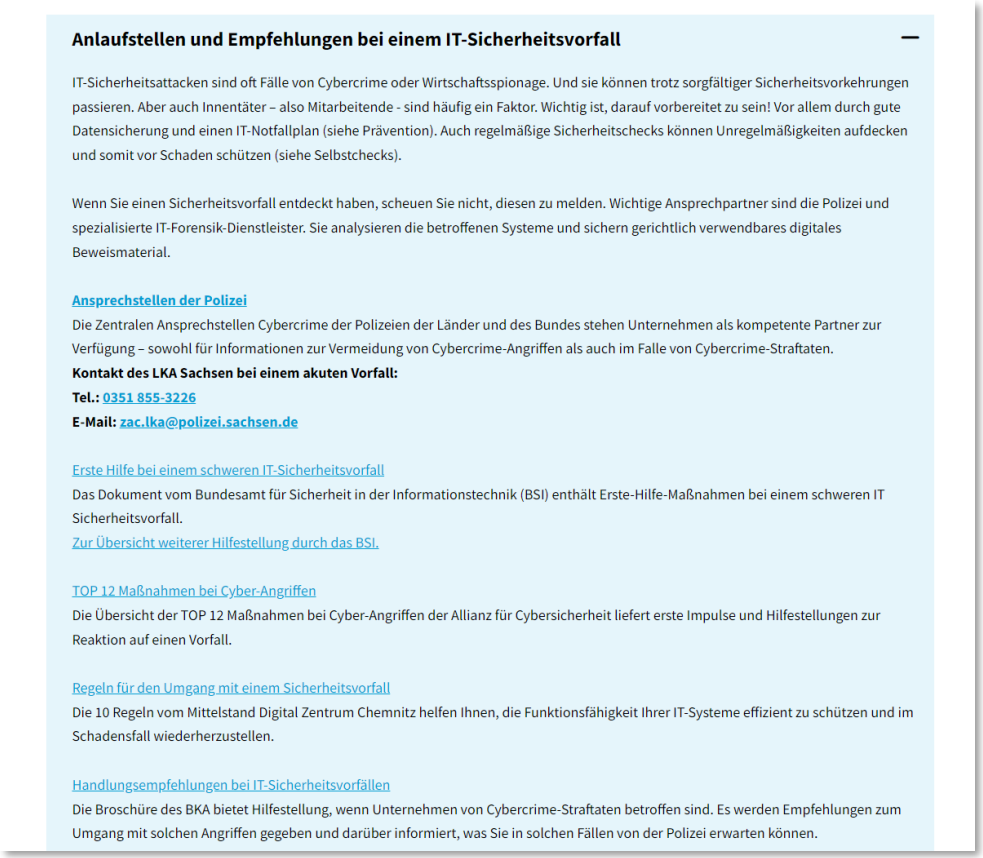
Informationsangebot auf unserer Website



Zusammenstellung von Material je Themenfeld

- **Anlaufstellen und Empfehlungen bei einem IT-Sicherheitsvorfall** +
- **Selbstchecks** +
- **Präventive Maßnahmen und Mitarbeitersensibilisierung** +
- **Wahl der IT-Dienstleister** +
- **Sicher in die Cloud** +
- **Anbieter für aktuelle Sicherheitswarnungen** +
- **Zusammenfassung Internetangebote** +
- **Fördermittel zur IT-Sicherheit** +

Beispiel Vorbereitung und Reaktion auf Vorfälle



Anlaufstellen und Empfehlungen bei einem IT-Sicherheitsvorfall

IT-Sicherheitsattacken sind oft Fälle von Cybercrime oder Wirtschaftsspionage. Und sie können trotz sorgfältiger Sicherheitsvorkehrungen passieren. Aber auch Innentäter – also Mitarbeitende - sind häufig ein Faktor. Wichtig ist, darauf vorbereitet zu sein! Vor allem durch gute Datensicherung und einen IT-Notfallplan (siehe Prävention). Auch regelmäßige Sicherheitschecks können Unregelmäßigkeiten aufdecken und somit vor Schaden schützen (siehe Selbstchecks).

Wenn Sie einen Sicherheitsvorfall entdeckt haben, scheuen Sie nicht, diesen zu melden. Wichtige Ansprechpartner sind die Polizei und spezialisierte IT-Forensik-Dienstleister. Sie analysieren die betroffenen Systeme und sichern gerichtlich verwendbares digitales Beweismaterial.

Ansprechstellen der Polizei
Die Zentralen Ansprechstellen Cybercrime der Polizeien der Länder und des Bundes stehen Unternehmen als kompetente Partner zur Verfügung – sowohl für Informationen zur Vermeidung von Cybercrime-Angriffen als auch im Falle von Cybercrime-Straftaten.
Kontakt des LKA Sachsen bei einem akuten Vorfall:
Tel.: 0351 855-3226
E-Mail: zac.lka@polizei.sachsen.de

Erste Hilfe bei einem schweren IT-Sicherheitsvorfall
Das Dokument vom Bundesamt für Sicherheit in der Informationstechnik (BSI) enthält Erste-Hilfe-Maßnahmen bei einem schweren IT Sicherheitsvorfall.
Zur Übersicht weiterer Hilfestellung durch das BSI.

TOP 12 Maßnahmen bei Cyber-Angriffen
Die Übersicht der TOP 12 Maßnahmen bei Cyber-Angriffen der Allianz für Cybersicherheit liefert erste Impulse und Hilfestellungen zur Reaktion auf einen Vorfall.

Regeln für den Umgang mit einem Sicherheitsvorfall
Die 10 Regeln vom Mittelstand Digital Zentrum Chemnitz helfen Ihnen, die Funktionsfähigkeit Ihrer IT-Systeme effizient zu schützen und im Schadensfall wiederherzustellen.

Handlungsempfehlungen bei IT-Sicherheitsvorfällen
Die Broschüre des BKA bietet Hilfestellung, wenn Unternehmen von Cybercrime-Straftaten betroffen sind. Es werden Empfehlungen zum Umgang mit solchen Angriffen gegeben und darüber informiert, was Sie in solchen Fällen von der Polizei erwarten können.

Beispiel Vorbereitung und Reaktion auf Vorfälle

Einstieg ins IT-Notfallmanagement für kleinere und mittelständische Unternehmen (KMU)

1. Vorbereitung

Die nachfolgenden Aufgaben sollten Sie bearbeiten, um im Fall der Fälle geeignet auf einen IT-Notfall vorbereitet zu sein:

- Bestimmen Sie Beauftragte für die Belange der IT-Sicherheit und des Notfallmanagements.
- Stellen Sie sicher, dass Ihnen Ihre individuellen Erstmaßnahmen bei IT-Vorfällen vorliegen (u. a. Alarmierungs- und Meldewege im Unternehmen).
- Identifizieren Sie zeitkritische Geschäftsprozesse und Assets (Kronjuwelen) und setzen Sie Schutzmaßnahmen für diese priorisiert um.
- Klären Sie mit Ihren IT-Dienstleistern, bei welcher Art von IT-Vorfällen diese unterstützen können.
- Identifizieren und kontaktieren Sie ggf. weitere IT-Dienstleister, die Sie bei der Bewältigung unterstützen können.
- Fertigen Sie eine Liste mit Ansprechpartnern und deren Erreichbarkeiten und Verfügbarkeiten.
- Legen Sie Regeln zur Kommunikation nach innen und außen fest, Stichwort: Presse- und Öffentlichkeitsarbeit.
- Implementieren Sie aktive Überwachungsmaßnahmen (Monitoring) für Ihre IT-Landschaft. Beachten Sie den Datenschutz.
- Üben Sie IT-Notfallszenarien.
- Lassen Sie Ihre IT-Infrastruktur auf Angreifbarkeit prüfen (Penetrationstests).
- Schulen und sensibilisieren Sie Ihr gesamtes Personals.
- Denken Sie an grundlegende Schutzmaßnahmen:
  - Installieren Sie regelmäßig und unverzüglich Patches und Sicherheitsupdates.
  - Setzen Sie Programme zum Schutz vor Schadsoftware ein und aktualisieren Sie diese regelmäßig.
  - Nutzen Sie Firewalls, um Ihre Netze und Rechner vor Angriffen von außen zu schützen.
  - Ändern Sie in jedem Fall Standard-Passwörter und nutzen Sie sichere Passwörter und, wenn möglich, Zwei-Faktor-Authentisierung.
  - Erstellen Sie regelmäßig Sicherheitskopien (Backups) Ihrer Daten, und testen Sie regelmäßig deren Wiederherstellung.
- Inventarisieren Sie Ihre IT-Infrastruktur (u.a. Netzplan).
- Vergeben Sie restriktive Benutzerrechte an Ihren Systemen.
- Vernetzen Sie Ihre Systeme restriktiv (Netzsegmentierung).
- Bereiten Sie Meldewege für externe Meldepflichten vor (Datenschutz, KRITIS etc.).

2. Bereitschaft

Um jederzeit einem IT-Notfall entgegnen zu können beachten Sie die nachfolgenden Punkte:

- Überprüfen Sie regelmäßig den Sicherheitsstatus Ihrer Systeme.
- Gewährleisten Sie, dass Ihr Personal den richtigen Ansprechpartner für IT-Notfälle kennt (Einsatz der IT-Notfallkarte). Bestimmen Sie einen angemessenen Erstkontakt für IT-Notfälle und gewährleisten Sie die Erreichbarkeit.

3. Bewältigung

Zur Bewältigung eines IT-Notfalls helfen Ihnen die folgenden Punkte:

- Kontaktieren Sie alle Ansprechpartner in der Organisation, die Sie zur Bewältigung brauchen.
- Befragen Sie betroffene Nutzer über Beobachtungen und Aktivitäten.
- Kontaktieren Sie IT-Dienstleister, die Ihnen bei der Bewältigung helfen können.
- Sammeln und sichern Sie Systemprotokolle, Logdateien, etc.
- Dokumentieren Sie Sachverhalte, die mit dem Notfall in Zusammenhang stehen könnten.
- Prüfen Sie Kontaktaufnahmen mit den ZACs der Polizeien, sowie freiwillige Meldungen an die ACS.
- Vermuten Sie als Urheber einen fremden Nachrichtendienst, wenden Sie sich an die Verfassungsschutzbehörden.
- Beachten Sie Meldepflichten.

4. Nachbereitung

Ein aufgetretener IT-Notfall muss auch nachbereitet werden. Hinweise geben die folgenden Punkte:

- Schließen Sie durch den IT-Notfall aufgedeckte Schwachstellen und Sicherheitslücken.
- Überwachen und Monitoren Sie Ihr Netzwerk und Ihre IT-Systeme im Nachgang besonders gründlich.
- Lessons Learned: Überprüfen Sie bestehende Regelungen, Prozesse und Maßnahmen, optimieren Sie diese gegebenenfalls.
- Halten Sie Ihre Dokumentationen zum Notfallmanagement auf dem aktuellen Stand.
- Entwickeln Sie Ihre IT-Sicherheitsarchitektur weiter.

Hinweis: Bei diesem Dokument handelt es sich um eine Kurzfassung des „Maßnahmenkatalog zum Notfallmanagement – Fokus IT-Notfälle" welcher weitere Erläuterungen und Verweise enthält.

Stand: Mai 2021

Disclaimer: Produkt einer Arbeitsgruppe deutscher Cyber-Sicherheitsorganisationen

Informationsangebot auf unserer Website

leipzig.ihk.de/it-sicherheit

Fördermittel

Fördermittel zur IT-Sicherheit

Ihre Investition zur Verbesserung der IT-Sicherheit im Unternehmen kann gefördert werden:

Förderprogramm "Digitalisierungszuschuss Sachsen"

Der Freistaat Sachsen unterstützt Digitalisierungsprojekte von sächsischen KMU. Dies umfasst auch die Verbesserung des Sicherheitsniveaus im Unternehmen. Ziel ist, vorhandene Engpässe und Lücken des eigenen Schutzniveaus zu erkennen und geeignete Maßnahmen im Zuge einer stringenten Schutzstrategie abzuleiten. Die Höhe des Zuschusses und der maximalen förderfähigen Ausgaben sind abhängig von der Unternehmensgröße.

Förderprogramm "go-digital"

Der Bund unterstützt kleine und mittlere Unternehmen der gewerblichen Wirtschaft bei Beratungsleistungen – auch zur IT-Sicherheit. Das Programm umfasst:

- Risiko- und Sicherheitsanalyse (Bewertung von Bedrohungen und möglichen Schwachstellen) der bestehenden oder neu geplanten betrieblichen IKT-Infrastruktur
- Maßnahmen zur Initiierung bzw. Optimierung von betrieblichen IT-Sicherheitsmanagementsystemen
- Vermeidung von wirtschaftlichen Schäden sowie Minimierung von Risiken durch den selbstständigen Betrieb von grundlegend erforderlichen IT-Sicherheitsmaßnahmen

Cybersicherheitstag in Leipzig

17. April 2024

Themenschwerpunkt: Cybersicherheitsvorfall

Cybersicherheitsnetzwerk

»Mit dem Aufbau eines starken Netzwerkes möchten wir Kräfte bündeln und gemeinsam mit unseren Partnern in Sachsen insbesondere den sächsischen Mittelstand (cyber)sicherer machen.«

Frauke Greven, Leiterin der Digitalagentur Sachsen über das »Cyber-Sicherheitsnetzwerk Sachsen«

https://www.cyber-sicherheitsnetzwerk.sachsen.de

Cyber-Sicherheitsnetzwerk – Digitale Rettungskette

Hotline BSI:
0800-274 1000

Service-Zeiten:
8 bis 18 Uhr

Weitere Unterstützungsmöglichkeiten

Mittelstand-Digital
Zentrum
Chemnitz

Fachbereich IT-Sicherheit und Datenschutz

Leistungen:

- Veranstaltungen (Webinare, Workshops, …)
- Individuelle Unterstützung
- Durchführung von IT-Sicherheitschecks (Schwachstellen-Scans, …)

Mittelstand-Digital Zentrum Chemnitz

IHK

Mittelstand-Digital Zentrum Chemnitz

- c/o tti Technologietransfer und Innovationsförderung Magdeburg GmbH
  Bruno-Wille-Straße 9
  39108 Magdeburg

Roland Hallau
0391 74435-24
rhallau@tti-md.de

Andreas Neuenfels
0391 74435-23
aneuenfels@tti-md.de

Dr. David Wagner
0391 74435-28
dwagner@tti-md.de

Mike Wäsche
0391 74435-34
mwaesche@tti-md.de

Mittelstand-Digital

Gefördert durch:
Bundesministerium für Wirtschaft und Klimaschutz
aufgrund eines Beschlusses des Deutschen Bundestages

Vielen Dank für Ihre Aufmerksamkeit.

Jenny Krick

Abteilung Digitalisierung, IT und Zukunft

0341 1267-1176

Jenny.krick@leipzig.ihk.de