POLIZEIDIREKTION
GÖTTINGEN

Cybercrime.

TIPPS UND POLIZEILICHE HINWEISE

Inhalt

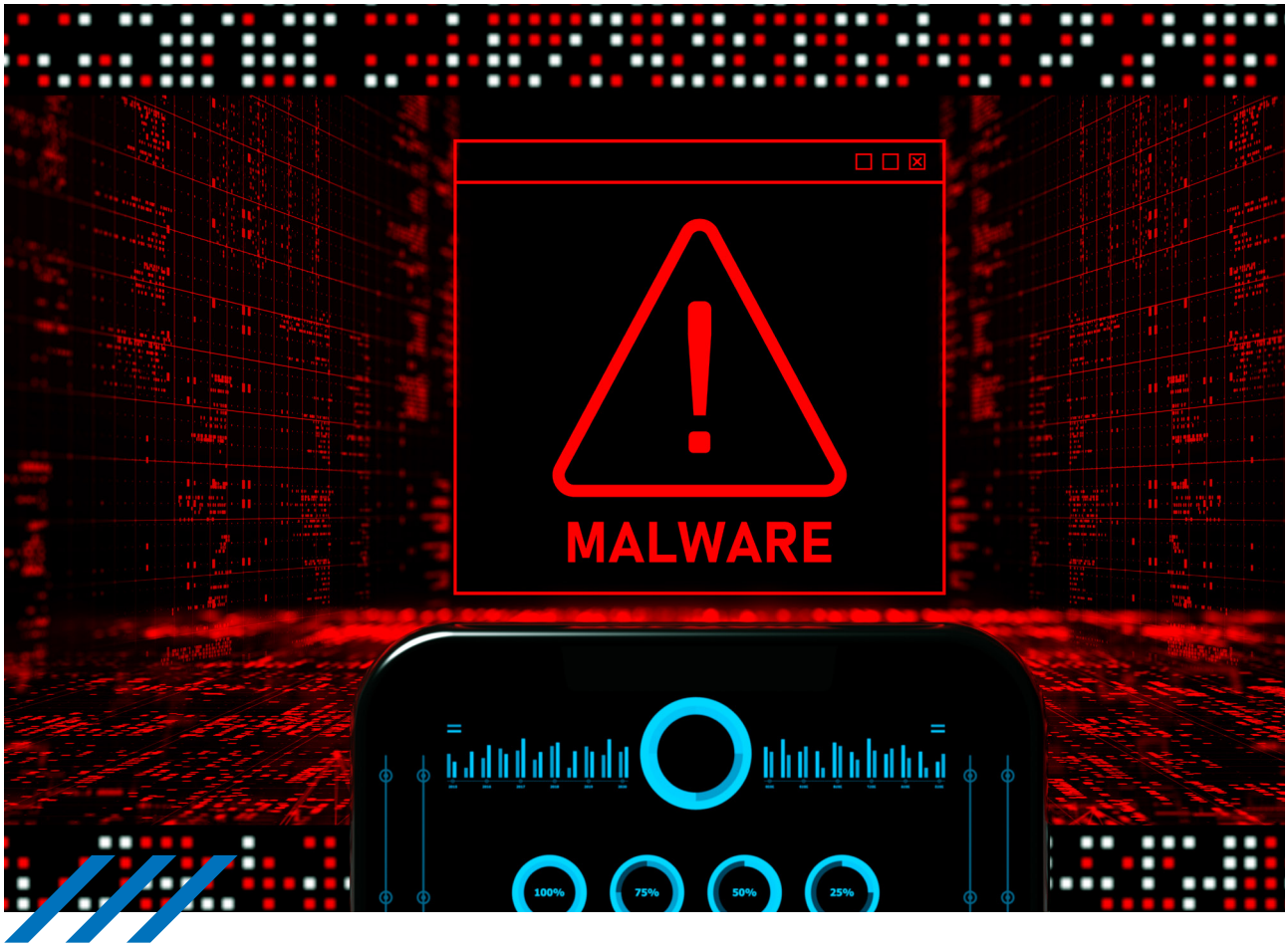
CYBERRISIKEN NEHMEN ZU 4

PRÄVENTION UND AUFKLÄRUNG 5

CYBER-ANGRIFF - WAS NUN? 6

POLIZEILICHE EMPFEHLUNGEN 7

Cyberrisiken nehmen zu



Cyber-Angriffe: Nicht ausschließlich ein Problem für Großkonzerne

Auch wenn Cyber-Kriminelle vorwiegend dort angreifen, wo es sich aus ihrer Sicht finanziell lohnt, und damit zielgerichtet wirtschaftlich starke Unternehmen, kritische Infrastruktur und öffentliche Einrichtungen in den Fokus nehmen, ist auch der Mittelstand erheblich betroffen.
Insbesondere Kleinstunternehmen, kleine und mittlere Unternehmen (KMU) sowie Freiberuflerinnen und Freiberufler verfügen nicht durchgängig über ein hinreichend ausgeprägtes Risikobewusstsein, die erforderliche Umsetzungskraft und IT-Fähigkeiten, um sich effektiv gegen Cyber-Angriffe zu schützen. Die Folgen von Cyber-Attacken sind oftmals immens. Insbesondere kriminelle Datenverschlüsselungen durch Ransomware, die mit Geldforderungen verbunden sind, oder DDoS-Angriffen zur Störung von IT-Systemen bzw. Websites verursachen häufig hohe Schäden.

Kümmern Sie sich um Ihre Daten – sonst tun es vielleicht Kriminelle!
Deshalb sollte ein bedarfsgerechtes IT-Sicherheitsmanagement Selbstverpflichtung und „ChefInnensache“ sein. Aber: Auch Privatpersonen werden nicht verschont und werden „Opfer“ von Cyberattacken und insbesondere Internetbetrügereien.

Prävention und Aufklärung

Auch individuell angepasste Schutzmaßnahmen bieten keine 100-prozentige Sicherheit und selbst Unternehmen mit einer ausgeprägten Cyber-Resilienz können schadensträchtige Cyber-Attacken erleiden. Die Vorbereitung auf den Krisenfall kann aber wirkungsvoll vor Datenverlust und schwerwiegenden Folgen durch Cyber-Angriffe schützen.

Die polizeiliche Aufgabe besteht neben der Prävention und damit Vorbeugung durch vorrangig (verhaltensorientierte) Informationen in der Aufklärung von Straftaten.

"Es hat Sie erwischt!" – unter diesem Motto hat das Bundeskriminalamt (BKA) einen informativen Flyer für Unternehmen herausgebracht und alle wichtigen Informationen für den Cyber-Angriffsfall zusammengefasst.

WEITERE INFORMATIONEN

Für Unternehmen, Behörden und Verbände in Niedersachsen:

Landeskriminalamt Niedersachsen (LKA NI):

Zentrale Ansprechstelle für die Wirtschaft (ZAC)

Bundeskriminalamt:

Handlungsempfehlungen für die Wirtschaft

Cyber-Angriff! Was nun?

WEITERFÜHRENDE INFORMATIONEN DER POLIZEI:

Landeskriminalamt Niedersachsen
Ratgeber Internetkriminalität:

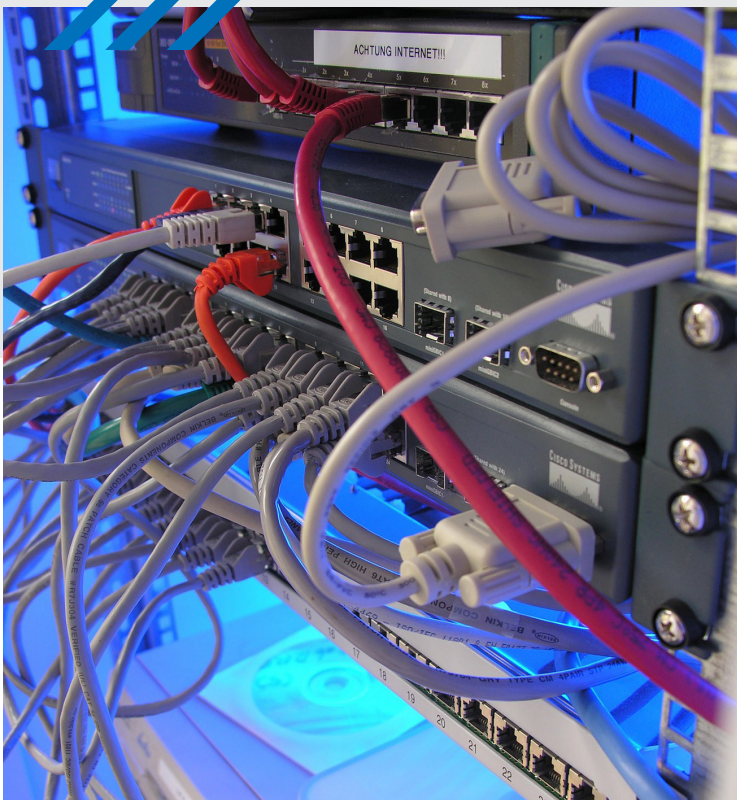
Bundeskriminalamt (BKA)
Informationen zum Thema Cybercrime:

Bundesamt für Sicherheit in der Informationstechnik (BSI)
Informationen unter anderem zum IT-Grundschutz:

Bundesamt für Sicherheit in der Informationstechnik (BSI)
ATP-Response-Liste

Bitte erstatten Sie eine Anzeige!
Um strafrechtliche Ermittlungen bei Cyber-Kriminalität führen zu können, ist die Polizei darauf angewiesen, möglichst früh von Straftaten zu erfahren. Oftmals werden Cyber-Taten jedoch gar nicht angezeigt. Das aufgrund von Studien anzunehmende Dunkelfeld polizeilich nicht bekannt gewordener Straftaten ist in diesem Deliktsbereich enorm. Zur langfristigen Bekämpfung ist jedoch ein möglichst umfassendes Bild von der Cybercrime-Lage erforderlich, zu dem die Daten aus Strafverfahren beitragen. Die Gründe für eine Nichtanzeige sind vielschichtig und reichen von der Sorge um Reputationsverlust bis zur irrigen Annahme, dass solche Taten nicht verfolgt würden. Wichtig zu wissen ist, dass die Polizei vertrauensvoll mit geschädigten Unternehmen und Privatpersonen umgeht und unternehmerische Maßnahmen beispielsweise zur Datenrettung nicht behindert. Für eine Schadensbeseitigung etwa durch Datenwiederherstellung oder für die Durchsetzung zivilrechtlicher Ansprüche ist die Polizei übrigens nicht zuständig.

Wo kann ich eine Strafanzeige bei der Polizei erstatten?
Hilfestellungen für Unternehmen, Behörden und Ver-



bände in Niedersachsen bietet die „Zentrale Ansprechstelle Cybercrime (ZAC)“ des Landeskriminalamtes Niedersachsen. Die ZAC ist die erste Ansprechpartnerin für Wirtschaftsunternehmen. Von hier werden erste Maßnahmen empfohlen und/oder initiiert. Strafanzeigen können aber auch bei jeder anderen Polizeidienststelle erstattet werden. Eine, bei akuten Cyber-Angriffen aufgrund Zeitverzuges jedoch nicht favorisierte Möglichkeit, bietet auch die Online-Wache www.onlinewache.polizei.niedersachsen.de.

Polizeiliche Empfehlungen

Digitale Spuren können wichtige Ansätze für die Ermittlungsarbeit geben und ggf. Rückschlüsse auf die Täter ermöglichen. Cybercrime ist oftmals ein Massenphänomen. Die Erkenntnisse einzelner Taten können zu einem Gesamtbild führen, das für die Aufklärung wichtig ist. Da Cyber-Kriminelle oftmals weltweit agieren, wird ein einzelner Fall nicht selten im Kontext betrachtet und wird Gegenstand zentraler Ermittlungen in Zusammenarbeit mit nationalen und internationalen Sicherheitsbehörden.

Die schnelle Kontaktaufnahme zur Polizei ist äußerst bedeutsam. Denn: So können Absprachen zu Datensicherungen als Beweismittel abgestimmt und beweiskräftig durchgeführt werden. Sind Rechner bereits neu installiert, sind wesentliche Ermittlungsansätze unwiederbringlich vernichtet. Insbesondere das System, das als Schwachpunkt bei einem Cyberangriff ausgenutzt worden ist, sollte zwar außer Betrieb gesetzt werden, aber noch vorgehalten werden.

Deshalb:

- Bitte zögern Sie nicht und nehmen Sie sofort mit der Polizei Kontakt auf (z.B. mit der Zentralen Ansprechstelle Cybercrime im Landeskriminalamt Niedersachsen als Single Point of Contact).
- Wenn möglich, vergewissern Sie sich, was angegriffen wurde: Server eines IT-Systems, ein PC oder ein einzelner Account.
- Bitte trennen Sie – wenn möglich und vertretbar – IT-Gerät(e) vom Internet!
- Bitte nehmen Sie keine Löschungen oder Deinstallationen vor bzw. behalten Sie noch eine Kopie für spätere Ermittlungen.
- Bitte bedienen Sie Meldewege im Unternehmen, gegenüber der niedersächsischen Datenschutzbehörde und in besonderen Fällen dem Bundesamt für Sicherheit in der Informationstechnik (BSI).
- Bitte benennen Sie der Polizei einen kompetenten Ansprechpartner (IT-Dienstleister, eigene IT-Abteilung, beauftragtes IT-Unternehmen).
- Schauen Sie sich schon vor einem Angriff nach geeigneten Forensik-Dienstleistern um, die Ihnen bei einem Angriff weiterhelfen können und erstellen Sie einen IT-Notfallplan.
- Die Onlinewache der Polizei Niedersachsen ist insbesondere für Bürgerinnen und Bürger geeignet, die Opfer eine Onlinestraftat geworden sind.

Herausgeber: Polizeidirektion Göttingen, Dezernat 11
Layout und Redaktion: Pressestelle der Polizeidirektion Göttingen
Grafiken: www.pixabay.de & istock/AHMET YARALI/CROCOTHERY/Olemedia/matejmo

POLIZEIDIREKTION
GÖTTINGEN