Sofortmaßnahmen bei Cyber-Angriffen

Ermittlungszusammenarbeit mit den Strafverfolgungsbehörden

gdv.de

FOTO: ISTOCK

Landeskriminalamt Nordrhein-Westfalen

POLIZEI
Nordrhein-Westfalen
Landeskriminalamt

Staatsanwaltschaft Köln

Staatsanwaltschaft Köln
Zentral- und Ansprechstelle Cybercrime
Nordrhein-Westfalen - ZAC NRW

LKRZV Krisenreaktionszentrum für IT-Sicherheit

LKRZV GmbH
IT-SICHERHEIT FÜR VERSICHERUNGEN

FOTO: CDU OBERBERG

Der Schutz der Daten der Versicherten genießt ohne Zweifel bei der deutschen Versicherungswirtschaft einen hohen Stellenwert! Denn Daten sind heutzutage in einigen Branchen wertvoller als Bargeld. Und das gilt bei der Versicherungswirtschaft für geradezu jeden Bereich. Es betrifft nämlich nicht nur Kontoverbindungen und Passwörter für den E-Mailverkehr. Hier geht es um Krankendaten, Schadenunterlagen oder auch um klassische Betriebsgeheimnisse. Virtuelle Angriffe sind daher eine ganz reale Gefahr für eine ganze Branche!

Deswegen ist es wichtig, dass die Versicherungswirtschaft eng und vertrauensvoll mit der Justiz zusammenarbeitet – und zwar nicht erst, wenn die Tat öffentlich geworden ist. Denn je früher wir als Justiz beteiligt werden, umso besser können wir helfen, den Schaden zu begrenzen und natürlich in erster Linie die Tat aufklären. Uns ist dabei bewusst, dass jeder erfolgreiche Cyber-Angriff auch ein Angriff auf den guten Ruf des betroffenen Unternehmens ist. Doch gerade die erfolgreiche Strafverfolgung kann ein wesentlicher Bestandteil Ihrer Krisenkommunikation werden.

Deswegen versteht sich die nordrhein-westfälische Justiz in diesen Fällen auch als Dienstleister, soweit das mit den Aufgaben der Strafverfolgung zu vereinbaren ist. Die ZAC steht Ihnen sieben Tage die Woche rund um die Uhr als kompetenter Ansprechpartner zur Verfügung.

PETER BIESENBACH
Minister der Justiz des Landes Nordrhein-Westfalen

FOTO: LVM

Die Digitalisierung schreitet unaufhaltsam voran und bringt viele Vorteile mit sich: Prozesse beschleunigen sich, neue Geschäftsmodelle entstehen, die Kommunikation mit den Kunden wird schneller und direkter. Für die Versicherungswirtschaft sind aber auch Sicherheitsaspekte und der unbedingte Schutz der Kundendaten essentiell.

Denn die Digitalisierung birgt auch Risiken. Cyber-Kriminelle versuchen etwa, durch Angriffe oder Erpressung an die Daten der Unternehmen zu gelangen. Dies gilt es zu bekämpfen – vorausschauend ebenso wie bei einem akuten Angriff.

Präventiv hat die deutsche Versicherungswirtschaft in den vergangenen Jahren mit dem Aufbau des Lage-und Krisenreaktionszentrums für IT-Sicherheit (LKRZV) bereits hervorragende Arbeit geleistet. Jetzt möchten wir unsere Kooperation mit den Strafverfolgungsbehörden weiter intensivieren und freuen uns, gemeinsam mit dem Landeskriminalamt und der Zentral- und Ansprechstelle Cybercrime (ZAC NRW) einen Krisenplan vorlegen zu können, der unter der Schirmherrschaft des nordrhein-westfälischen Ministers der Justiz erarbeitet wurde. Es ist unser erklärtes Ziel, diesen Krisenplan fortlaufend weiterzuentwickeln und durch Vernetzung der verantwortlichen Stellen Krisen auf Landes- und Bundesebene effektiv zu bewältigen.

WERNER SCHMIDT
Vorsitzender des Ausschusses Betriebstechnik, Digitalisierung und IT, Gesamtverband der Deutschen Versicherungswirtschaft e.V.

CYBER-SICHERHEIT – EIN KRITISCHER ERFOLGSFAKTOR

Als Teil der Kritischen Infrastrukturen muss die deutsche Versicherungswirtschaft weitreichende Anforderungen an die Sicherheit ihrer IT-Systeme erfüllen. Dazu zählt in erster Linie der präventive Schutz vor externen und internen Angriffen. Im Krisenfall gilt es für Versicherungsunternehmen, schnell geeignete Gegenmaßnahmen zu ergreifen und zeitnah die Strafverfolgung mit dem Ziel einer Täterermittlung einzuleiten. Um dies zu gewährleisten, sollen zukünftig durch einen engeren und schnelleren Informationsaustausch zwischen den betroffenen Versicherungsunternehmen und den Strafverfolgungsbehörden die Ermittlungsarbeiten wirksamer unterstützt werden.

DIESES INFORMATIONSBLATT BIETET HIERFÜR ERSTE HILFESTELLUNGEN:

Unternehmen können Krisensituationen wie einen Cyber-Angriff ohne eine vorausschauende Vorbereitung nicht erfolgreich bewältigen. Anhand prognostischer Szenarien sollten die in einem Unternehmen bei der Krisenbewältigung einzubindenden Personen, die Meldewege und die Entscheidungsbefugnisse in einem Cyber-Notfallplan festgelegt werden. Nur so lässt sich die erforderliche Handlungsschnelligkeit gewährleisten. Die gebotene Handlungssicherheit lässt sich durch die entsprechende Einübung der Abläufe im Krisenfall trainieren.

Wesentlicher Bestandteil der Krisenbewältigungsstrategie sollte die unverzügliche Erstattung einer Strafanzeige sein. Die Strafverfolgungsbehörden sind professionelle Krisenmanager, die betroffene Unternehmen unterstützen können. Die Sicherung von Beweismitteln ermöglicht die Ermittlung des Tathergangs. Sie erfolgt unter Berücksichtigung der Unternehmensinteressen in Abstimmung mit dem geschädigten Unternehmen.

Die Strafverfolgungsbehörden streben eine effektive und vertrauensvolle Kooperation an. Dazu gehört auch ein koordiniertes Reputations- und Öffentlichkeitsmanagement. Interne Ermittlungsressourcen des angegriffenen Unternehmens können in die Ermittlungen einbezogen werden. Hier empfiehlt sich eine frühzeitige Abstimmung des Vorgehens im Einzelfall.

Wirksame Krisenbewältigung und effektive Strafverfolgung sind zwei ineinandergreifende Komponenten. Nur durch das Aufhellen des Dunkelfeldes und die Verurteilung von Tätern lässt sich das Geschäftsmodell der Cyber-Kriminellen nachhaltig bekämpfen. Die Strafanzeige ermöglicht den Rückfluss behördlicher Erkenntnisse aus dem Ermittlungsverfahren zu geschädigten oder gefährdeten Unternehmen. Justiz und Polizei haben spezialisierte Cybercrime-Dienststellen geschaffen, die den Unternehmen als zentrale Ansprechpartner zur Verfügung stehen.

ZUSTÄNDIGKEITEN UND REAKTIONEN IM KRISENFALL

Das Hauptkriterium für eine effektive Strafverfolgung bei Cyber-Angriffen ist schnelles Handeln. Daher sollten bereits vorab Maßnahmen ergriffen und Zuständigkeiten geklärt werden, um im Angriffsfall sicher und schnell handeln zu können. Hierzu gehört die Erstellung des Krisenplans und entsprechende regelmäßige Übungen.

Unter anderem sind folgende Fragen vor dem Ernstfall zu klären:

1 ZUSTÄNDIGKEITEN KLÄREN

- ☐ Interne Abstimmungsprozesse regeln:
  - Management
  - Rechtsabteilung
  - IT
  - Sicherheitsbeauftragte/r
  - Datenschutzbeauftragte/r
  - Pressestelle
  - Betriebsrat
- ☐ Rechtliche Zuständigkeit für Strafanzeigenerstattung klären.

2 KRISENFALL DARLEGEN

- ☐ Möglichst genaue Vorfallbeschreibung verfassen.
- ☐ Daten sichern und bereitstellen, ggf. in Absprache mit der/dem Datenschutzbeauftragten und dem Betriebsrat.
- ☐ Beweissicherung in Absprache mit den Ermittlungsbehörden vornehmen (*bspw. Logfiles*).

3 REAKTIONEN KOORDINIEREN

- ☐ Verhaltens- und Kommunikationsrichtlinien für Mitarbeiter und Führungskräfte erstellen.
- ☐ Ermittlungsbehörden Zutritt zum Gebäude sowie Zugang und Zugriff zu den betroffenen IT-Systemen gewähren.
- ☐ Strategie für Reputations- und Öffentlichkeitsmanagement erarbeiten, ggf. in Abstimmung mit den Ermittlungsbehörden.

In Nordrhein-Westfalen sind die zuständigen Behörden das Cybercrime-Kompetenzzentrum des Landeskriminalamtes Nordrhein-Westfalen und die bei der Staatsanwaltschaft Köln angesiedelte und landesweit zuständige Zentral- und Ansprechstelle Cybercrime Nordrhein-Westfalen (ZAC NRW). Beide sind im Cyber-Krisenfall jederzeit erreichbar.

Landeskriminalamt Nordrhein-Westfalen
Cybercrime-Kompetenzzentrum
Zentrale Ansprechstelle Cybercrime
Single Point of Contact

Völklinger Straße 49 | 40221 Düsseldorf
Tel.: +49 211 939 4040
Fax: +49 211 939 194040
cybercrime.lka@polizei.nrw.de

POLIZEI Nordrhein-Westfalen Landeskriminalamt

Staatsanwaltschaft Köln
Zentral- und Ansprechstelle Cybercrime
Nordrhein-Westfalen - ZAC NRW -

Am Justizzentrum 13 | 50939 Köln
Tel.: +49 221 477 4922 (24/7-Hotline)
Fax: +49 221 477 4400
zac@sta-koeln.nrw.de

Staatsanwaltschaft Köln
Zentral- und Ansprechstelle Cybercrime
Nordrhein-Westfalen - ZAC NRW

Bei versicherungsspezifischen Fragen zur IT-Sicherheit wenden Sie sich bitte an:

LKRZV
Krisenreaktionszentrum für IT-Sicherheit der deutschen Versicherungswirtschaft

(Erreichbarkeit 24/7): krisenreaktionszentrum@gdv.de

während der Geschäftszeiten:
Tel.: +49 30 2020 5050
Fax: +49 30 2020 6050

LKRZV GmbH
IT-SICHERHEIT FÜR VERSICHERUNGEN