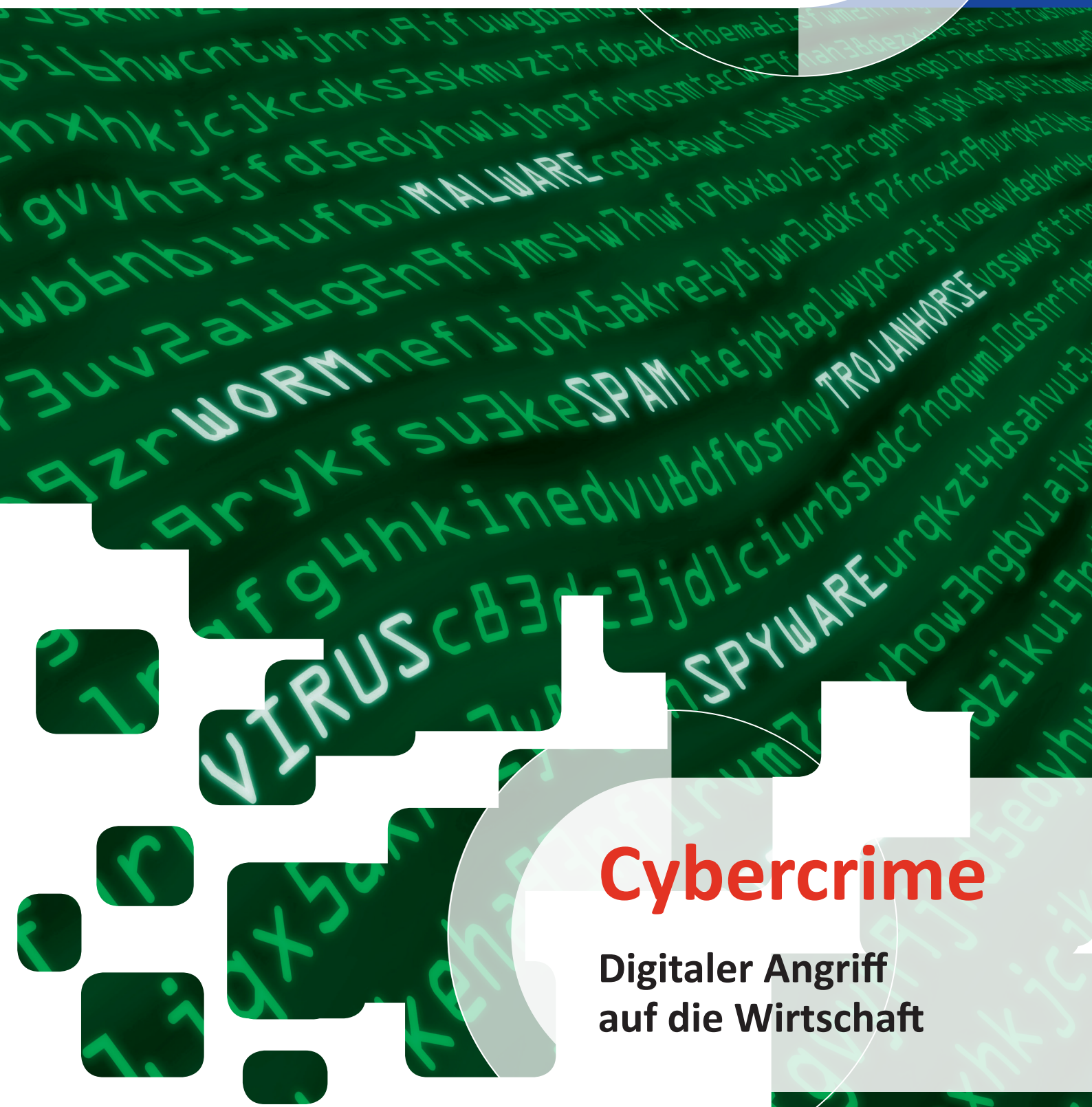
Leseprobe

POLIZEI
DEIN PARTNER
Gewerkschaft der Polizei



Cybercrime

Digitaler Angriff auf die Wirtschaft

www.vdp-polizei.de

POLIZEI DEIN PARTNER

Gewerkschaft der Polizei

Impressum

Verantwortlich für den redaktionellen Teil:
pressto gmbh – agentur für medienkommunikation, Köln;

Fotos Titel/Innentitel: J.R. Bale/Fotolia.com /
Jakub Jirsák/Fotolia.com

VERLAG DEUTSCHE POLIZEILITERATUR GMBH
Anzeigenverwaltung
Ein Unternehmen der Gewerkschaft der Polizei

Forststraße 3 a • 40721 Hilden
Telefon 0211 7104-0 • Telefax 0211 7104-174
av@vdp-polizei.de

Geschäftsführer: Bodo Andrae, Joachim Kranz
Anzeigenleiterin: Antje Kleuker

Gestaltung und Layout: Jana Kolfhaus

Anzeigensatz und Druck:
Griebsch & Rochol Druck GmbH & Co. KG, Hamm

12/2018/21

www.vdp-polizei.de

Cybercrime

Vertrauen schafft Sicherheit

Das Thema Cybercrime beschäftigt die Polizei in zunehmendem Maße. Ein großes Problem dabei: Viele Unternehmen, die von Internetkriminellen angegriffen werden, wenden sich im Anschluss nicht an die Polizei. Die Gründe für das geringe Anzeigeverhalten sind vielfältig, wie eine Unternehmensbefragung der IHK Nord zur „Betroffenheit der norddeutschen Wirtschaft von Cybercrime“ im Jahr 2013 zeigt: 54 Prozent der befragten und von Cybercrime betroffenen Unternehmen geben darin an, dass sie den Anzeigeaufwand als zu groß erachten. 30 Prozent der Unternehmen haben Zweifel am Ermittlungserfolg der Behörden und 22 Prozent antworteten, dass sie nicht wüssten, an wen sie sich wenden sollten.

Steffen Rösemann von der Zentralen Ansprechstelle Cybercrime im LKA Niedersachsen

Die Umfrage zeigt außerdem: Jedes dritte Unternehmen in Norddeutschland ist Opfer von Cyberattacken. Betreibt das Unternehmen zudem einen Webshop, vergrößert sich die Angriffsfläche für die Cyberkriminellen. In der Regel haben weder Branchenzugehörigkeit noch Unternehmensgröße oder IT-Nutzungsverhalten wesentlichen Einfluss auf die Angriffswahrscheinlichkeit. Die überwiegende Zahl der Angriffe erfolgt auf Server oder stationäre Endgeräte der Unternehmen – und zwar meistens durch Schadsoftware. „Die Umfrage-Ergebnisse haben unter anderem dazu geführt, dass wir unsere Angebote im Bereich Internetsicherheit für Wirtschaftsunternehmen weiter ausgebaut haben“, erklärt Steffen Rösemann von der „Zentralen Ansprechstelle Cybercrime“ (ZAC) im Landeskriminalamt Niedersachsen.

ZAC unterstützt und berät

Nicht zuletzt aufgrund der hohen Dunkelziffer im Bereich Cyberkriminalität wurde bereits im August 2011 die „Zentrale Ansprechstelle Cybercrime“ im LKA Niedersachsen eingerichtet. Die Fachstelle ist Ansprechpartner für Wirtschaftsunternehmen – sowohl bei allgemeinen Fragen rund um das Thema Cybercrime als auch bei konkreten Vorfällen. Die ZAC unterstützt die Firmen etwa bei der Entwicklung von IT-Sicherheitskonzepten oder durch Beratungsgespräche und -veranstaltungen, die zum Teil auch bei den Firmen selbst stattfinden. „Wichtig ist, dass wir als Polizei Vertrauen zu den Unternehmen aufbauen, damit sie uns als wichtigen Partner anerkennen und im Ernstfall auch bereit sind, sich an uns zu wenden“, erklärt Rösemann das Konzept.

Zertifizierte IT-Sicherheitsdienstleister

Das Bundesamt für Sicherheit in der Informationstechnik bietet auf seiner Webseite www.allianz-fuer-cybersicherheit.de unter dem Reiter „Informationspool“ eine Liste mit zertifizierten IT-Sicherheitsdienstleistern. Die Zertifizierung gewährleistet, dass sich die Anbieter durch Zuverlässigkeit und Unabhängigkeit sowie Fachkompetenz und Qualität der Dienstleistung auszeichnen.

Informationsveranstaltungen bauen Hemmschwellen ab

Die IHK Nord lädt dazu regelmäßig ihre Mitglieder zu Informationsveranstaltungen ein, auf denen die Cybercrime-Experten des LKA wertvolle Tipps rund um das Thema Internetsicherheit geben. Ein weiterer wichtiger Programmpunkt: Die Experten klären die Teilnehmer über das polizeiliche Vorgehen bei Ermittlungen in Fällen von Cybercrime auf. „Viele denken, dass unsere Ermittlungen nach einem Vorfall den Betriebsablauf stören und es so noch zu weiteren Beeinträchtigungen kommt. Das ist nicht der Fall. Wir entwickeln gemeinsam mit den IT-Sicherheitsbeauftragten ein Konzept, das auf der einen Seite für das Ermittlungsverfahren beweissichernd und auf der anderen Seite für das Unternehmen schonend für den normalen Geschäftsbetrieb ist“, betont Steffen Rösemann. Ziel sei es, Hemmschwellen gegenüber der Polizei ab- und Vertrauen aufzubauen. „Wir können nur Vertrauen gewinnen, wenn wir auf die Unternehmen zugehen und ihnen erklären, was wir machen und wie die Abläufe sind“, so der Cybercrime-Spezialist. Auch für die Außendarstellung der Polizei seien diese Informationsveranstaltungen wichtig, denn so könne man zeigen, dass die Polizei gegen solche Angriffe durchaus gewappnet sei und auch über das nötige Know-how verfüge. „Durch unser professionelles Auftreten auf den Veranstaltungen zeigen wir, dass die Unternehmen im Ernstfall bei der Polizei gut aufgehoben sind“, so Rösemann. Die positive Folge: Im Anschluss an die Veranstaltungen wendeten sich viele der Teilnehmer mit ihren individuellen Fragen an die Zentrale Ansprechstelle Cybercrime.

Der „Ratgeber Internetkriminalität“

Auf der Webseite www.polizei-praevention.de gibt das LKA Niedersachsen zudem wichtige Tipps und Hilfestellungen rund um Cybercrime. Außerdem hat der Nutzer die Möglichkeit, direkten Kontakt zu den Experten aufzunehmen und Fragen zu stellen. „Eigentlich war der Webauftritt ursprünglich für Wirtschaftsunternehmen gedacht. Mittlerweile wird er aber auch von Bürgern und Bürgerinnen genutzt, die sich zu dem Thema Cyberkriminalität schlau machen wollen“, erklärt Steffen Rösemann. Auf der Seite werden zum Beispiel die verschiedenen Cybercrime-Phänomene erklärt und man erhält Tipps, wie man sich davor schützen kann. „Wir haben außerdem ein

Phishing-Mail-Konto eingerichtet, an das Nutzer die bei ihnen eingegangenen Betrugsmails schicken können. Wir können dann neue Phishing-Wellen frühzeitig erkennen und davor warnen“, so der Cybercrime-Spezialist.

LKA-Projekt: Auffinden von Sicherheitslücken

Die Beschäftigten der ZAC im LKA Niedersachsen suchen auch selbst aktiv nach Schwachstellen auf den Webseiten von Wirtschaftsunternehmen. Das Ziel: Die Unternehmen sollen auf gefährliche Sicherheitslücken aufmerksam gemacht werden, damit die Schwachstellen schnellstmöglich geschlossen werden können – noch bevor sie in den Fokus von Cyberkriminellen geraten. „Dieser „Service“ ist als Awareness-Projekt gedacht, um die Aufmerksamkeit der Unternehmen auf dieses wichtige Thema zu lenken. Es ersetzt aber nicht die so genannten Penetrationstests professioneller IT-Dienstleister, um Schwachstellen aufzufinden“, betont Rösemann. Auch würden Webseiten dabei nie gehackt, denn das sei illegal und aus diesem Grund auch der Polizei nicht erlaubt. Das Feedback der Unternehmen, deren Webseiten auf Schwachstellen überprüft werden, ist dabei durchweg positiv: „Die Unternehmen wissen es zu schätzen, dass wir in diesem Bereich Kompetenz aufgebaut haben und sind dankbar, wenn wir sie auf vorhandene Lücken hinweisen – denn auch das schafft Vertrauen“, weiß der IT-Experte.

Risiko-Analyse wichtig für Unternehmen

Um sein Unternehmen gegen Cyberkriminelle zu schützen, muss langfristig geplant und sinnvoll investiert werden. Dazu ist in der Regel die Beratung eines IT-Dienstleisters notwendig, der das Unternehmen auf seine Schwachstellen hin analysiert. „Man muss sich immer fragen: Was ist das schlimmste, was meinem Unternehmen passieren kann? Dass der Webshop ausfällt? Dass Kundendaten verlorengehen? In diesen Bereichen sollte man anfangen, die Sicherheit zu verstärken – und von dort aus weiter ausbauen“, erklärt Steffen Rösemann. Auch die Schwachstelle Mensch sei in diesem Zusammenhang nicht zu unterschätzen. Mithilfe von Social-Engineering-Methoden entlocken Cyberkriminelle Mitarbeitern vermeintlich unwichtige Informationen – die kombiniert wiederum wichtiges Firmenwissen preisgeben können. „Wie der bekannte ehemalige US amerikanische Hacker Kevin Mitnick schon sagte: Wenn man es schafft, an sieben unwichtige Informationen zu gelangen, dann ergeben diese zusammen am Ende eine wichtige Information“, so Rösemann. Daher seien Awareness-Schulungen für Beschäftigte ebenso wichtig, wie technische Vorkehrungen. *sw*

Die Hotlines der „Zentralen Ansprechstellen Cybercrime“ in den Landeskriminalämtern:

LKA Baden-Württemberg: Tel. 0711 – 54012444
LKA Bayern: Tel. 089 – 1212-3300
LKA Berlin: Tel. 030 – 4664 – 924924
LKA Brandenburg: Tel. 03334 – 388-8686
LKA Bremen: Tel. 0421 – 3623853
LKA Hamburg: Tel. 040 – 4286-75455
Hessisches Landeskriminalamt (HLKA): Tel. 0611 – 833377
LKA Mecklenburg-Vorpommern: Tel. 03866 – 644545
LKA Niedersachsen: Tel. 0511 – 26262-3804
LKA Nordrhein-Westfalen: Tel. 0211 – 9394040
LKA Rheinland-Pfalz: Tel. 06131 – 652565
Landespolizeipräsidium Saarland: Tel. 0681 – 9620
LKA Sachsen: Tel. 0351 – 855-3226
LKA Sachsen-Anhalt: Tel. 0391 – 2502244
LKA Schleswig-Holstein: Tel. 0431 – 1604545
LKA Thüringen: Tel. 0361 – 3411425