



Internet-Kriminalität: Unterschätzte Gefahren aus dem weltweiten Netz

Die Internet-Kriminalität (Cybercrime) ist auf dem Vormarsch. Dabei sehen sich Nutzer und Ermittlungsbehörden international vernetzten Kriminellen und Hackergruppen, aber auch Angriffen ausländischer Nachrichtendienste gegenüber.

Cybercrime ist ein fester Bestandteil der Wirtschaftskriminalität geworden. Nach Erhebungen des Bundeskriminalamtes (BKA) sind 2010 die in diesem Bereich registrierten Internet-Delikte auf über 31.000 gestiegen (+ 190 Prozent). Die Bedrohungslage unterstreicht auch eine Studie der Wirtschaftsprüfungsgesellschaft KPMG. Demnach gingen bei über der Hälfte

aller Unternehmen, die Opfer von Wirtschaftskriminalität wurden, die Schäden auf elektronische Angriffe, z. B. der organisierten Kriminalität, zurück. Im Vergleich zum Jahr 2006 hat sich der Wert damit mehr als verdoppelt. Ziel sind neben großen Unternehmen vor allem kleinere und mittelständische Firmen. Sie verfügen über begehrtes Know-how, vernachlässigen aber oft die Sicherheit. Gefahren gehen zudem von ausländischen Nachrichtendiensten und Hackergruppen aus. Der Gesamtschaden aller mit Internet-Kriminalität verbundenen Fälle summiert sich in Deutschland laut „Lagebild Cybercrime“ auf zirka 61,5 Millionen

Euro (+ 66 Prozent). Dabei wurden Zugangsdaten von insgesamt sieben Millionen Usern ausspioniert – fast doppelt so viele wie ein Jahr zuvor.

Besonders stark nahmen die Delikte beim Online-Banking sowie durch digitale Erpressung zu, bei der „Lösegeld“ beispielsweise für die Nichtweitergabe gestohlener Daten verlangt wird.

„Diese Zahlen machen deutlich, dass die Sicherheitsanstrengungen weiter verstärkt werden müssen“, sagt Hans-Helmut Janiesch, Mitglied im KÖTTER Sicherheitsbeirat und Leitender Polizeidirektor i. R. „Dies betrifft auch den Schutz kritischer Infrastrukturen.“

„Unternehmen müssen ihre Mitarbeiter stärker für die Cybercrime-Risiken sensibilisieren“

„Zeitbombe Internet“ lautet der Titel eines kürzlich erschienenen Buches. Realität oder Übertreibung?

Hans-Helmut Janiesch: Buchtitel wollen ja immer Neugier wecken und sind daher bewusst provokant gewählt. Der Titel macht aber zu Recht bewusst, welche erheblichen Risiken bereits heute im weltweiten Netz lauern und dass diese immer weiter wachsen.

Was verbirgt sich genau hinter dem Begriff Cybercrime?

Janiesch: Unter Cybercrime sind laut Bundeskriminalamt (BKA) alle Straftaten zu verstehen, die unter Ausnutzung moderner Informations- und Kommunikationstechnik (IuK) oder gegen diese begangen werden. Dies beinhaltet also sowohl Straftaten, bei denen IT für kriminelle Aktivitäten eingesetzt wird, als auch Angriffe gegen diese Infrastrukturen wie z. B. Hacking und Computersabotage.

... und hiervon sind immer mehr Nutzer betroffen ...

Janiesch: Laut Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e. V. – BITKOM – haben 70% aller User ab 14 Jahren negative Erfahrungen im Internet gemacht. Infektionen des PC mit Schadprogrammen stehen an erster Stelle, gefolgt von Betrugsdelikten, z. B. bei Online-Auktionen. Das Spektrum der Kriminalität reicht noch weiter: von der digitalen Erpressung, bei der z. B. „Lösegeld“ für das Unterlassen von Angriffen fällig wird, über Hackerattacken auf Netzwerke und mobi-

le Endgeräte wie Smartphones bis zum besonders hässlichen Deliktfeld der Kinderpornografie.

Weitere Schlagworte sind Carding, Botnetze und Scareware. Was verbirgt sich dahinter?

Janiesch: Beim Carding werden die gestohlenen Kreditkartendaten dazu genutzt, online Waren zu kaufen und weiterzuverkaufen. Stichwort Botnetze: Hierbei werden Tausende von Rechnern privater Nutzer infiziert, zusammengeschaltet und Unternehmen oder Institutionen mit Mailanfragen torpediert, unter deren Last die Server zusammenbrechen. Bei Scareware wiederum ist das Ziel, den Nutzer zu verunsichern und zu betrügen. Der Trick funktioniert z. B. über die fälschliche Info, der Rechner sei durch Viren verseucht. Einhergehend damit wird gegen Bezahlung eine vermeintliche Sicherheitssoftware angeboten. Diese ist entweder nutzlos und es geht ums Abkassieren. Oder sie ist infiziert und die Betreiber gelangen an Nutzerdaten.

... und die Schäden bei Unternehmen?

Janiesch: Gemäß dem kürzlich vom BKA vorgelegten Bundeslagebild wurde 2010 bei mehr als jedem vierten Fall von Wirtschaftskriminalität, dessen Gesamtschaden rd. 4,7 Milliarden Euro beträgt, das Internet als Tatmittel genutzt. Besonders alarmierend: Die Kriminellen folgen der veränderten Mediennutzung, zielen also außer auf Internetseiten und Netzwerke immer stärker auch auf mobile Endgeräte wie Smartphones etc. ab. Eine erhebli-

che Gefahr für die Unternehmen ist das Social Engineering. Dabei geht es darum, Firmenmitarbeiter ohne ihr Wissen „anzuzapfen“ bzw. illegal an sensible Daten zu gelangen, indem man die Beschäftigten unter Druck setzt oder ihre Hilfsbereitschaft ausnutzt.

Die Gefahren werden also in Zukunft weiter zunehmen?

Janiesch: Davon ist leider auszugehen. Dies verdeutlicht wohl nicht zuletzt die Tatsache, dass die NATO Cyberattacken – neben Raketenangriffen und terroristischen Akten – als eines von drei möglichen Bedrohungsszenarien der Zukunft definiert hat. Zudem lässt sich der Trend durch nüchterne Zahlen unterstreichen. Die Zahl der Nutzer, deren Zugangsdaten zu Online-Banking, E-Mail-Diensten etc. ausspioniert wurden, hat sich 2010 nahezu verdoppelt – auf rd. sieben Millionen Betroffene. Parallel nimmt der Umfang der Schadprogramme nach Erkenntnissen des Bundesamtes für Sicherheit in der Informationstechnik (BSI) rapide zu: Etwa alle zwei Sekunden entsteht eine neue Variante. Und das bei weiter steigender Nutzung insbesondere des mobilen Datenverkehrs.

Von wem gehen die Bedrohungen aus?

Janiesch: Die Delikte gehen von Internet-Kriminellen aus, die international vernetzt sind. Dabei agieren sie nach Erkenntnissen des BKA zumeist arbeitsteilig. Dies bedeutet: Sie begehen nicht nur selbst die Straftaten, sondern bieten auch Schadprogramme oder komplette kriminelle Infrastruktu-

ren in Foren zum Kauf an. Die organisierte Kriminalität macht sich Cybercrime zudem im Rahmen der Geldwäsche zunutze, indem sie auf betrügerisch erlangte Online-Banking-Daten zurückgreift.

In den Schlagzeilen waren zudem Hackerattacken.

Janiesch: Das trifft zu. Diese Internet-Piraten, von denen die Gruppierungen „Anonymous“ und „LulzSec“ in der Vergangenheit wohl am bekanntesten geworden sind, haben den „Krieg im Internet“ angekündigt. So wurden bereits die Internetseiten des US-Geheimdienstes und -Senats, der britischen Polizeibehörde, aber auch von Konzernen angegriffen. Die Ziele der Gruppierungen sind diffus. Einige führen den Kampf gegen die angebliche Beherrschung des Internets durch Behörden und Unternehmen. Andere verfolgen politische Ziele. Einer dritten Gruppe geht es darum, Sicherheitslücken aufzudecken.

Und Nachrichtendienste?

Janiesch: Die Angriffe mit nachrichtendienstlichem Hintergrund steigen nach Erkenntnissen des Bundesamtes für Verfassungsschutz beständig. Im Jahr 2010 wurden 2.108 elektronische Angriffe auf Bundesbehörden festgestellt. Dies bedeutet im Vergleich zum Vorjahr, als es 1.511 Delikte waren, einen Anstieg um 40 Prozent! Ziel ist es, an politische, wirtschaftliche und militärische Informationen zu gelangen.

Solche Angriffe scheinen sich somit zu lohnen, was im Umkehrschluss heißt: Die Sicherheitsmaßnahmen lassen teils noch zu wünschen übrig ...

Janiesch: Tatsächlich lassen hier einige Zahlen aufschrecken. Nach

wie vor ist jeder fünfte Nutzer ohne Virenschutz oder Firewall im Netz unterwegs. Auch bei der Unternehmenssicherheit gibt es Nachholbedarf. Die Umfrage von „Deutschland sicher im Netz“ unter rd. 1.400 meist kleineren Unternehmen ergab: Nur jedes vierte schult und informiert seine Mitarbeiter regelmäßig, nur jedes dritte hat ein IT-Sicherheitskonzept, das von der Geschäftsleitung getragen wird, 37% sichern ihre Daten nicht täglich, sieben Prozent sogar nie!

Was ist gerade für Unternehmen und Institutionen zu tun?

Janiesch: Grundlage ist – analog



Hans-Helmut Janiesch

Hans-Helmut Janiesch, Leitender Polizeidirektor/Kriminaldirektor i. R., war von 1998 bis 2007 Abteilungsleiter Gefahrenabwehr und Strafverfolgung des Polizeipräsidiums Essen. Als Gründungsmitglied der Sicherheitspartnerschaft Essen/Mülheim an der Ruhr verfügt der 64-Jährige über wichtige Erfahrungen mit Blick auf die Kooperation von Polizei und Sicherheitsunternehmen. Weiterer Schwerpunkt seiner Arbeit im KÖTTER Sicherheitsbeirat ist das Thema Aus- und Weiterbildung, dem er sich zuvor schon als nebenamtlicher Lehrbeauftragter an den Fachhochschulen Dortmund und Wuppertal gewidmet hat.

zu anderen Sicherheitsbereichen – ein umfassendes Sicherheitskonzept, das eine Risikoanalyse und die notwendigen Maßnahmen enthält. Beim Schutz der Rechner und Netzwerke durch Firewalls, Antivirenprogramme, Verschlüsselungstechnologien etc. müssen sämtliche Systeme einbezogen werden; also etwa auch PC zur Maschinensteuerung oder Anlagen, die zum Betrieb online sind.

Damit sind auch die so genannten kritischen Infrastrukturen besonders im Blickfeld.

Janiesch: Ihnen muss ganz besondere Aufmerksamkeit zukommen. Die in der Vergangenheit zu verzeichnenden Cyberangriffe auf Regierungs- und Behördennetzwerke verschiedener Länder, aber auch auf IT-Systeme wichtiger Infrastrukturen unterstreichen dies in aller Deutlichkeit.

Erhebliche Relevanz hat zudem das Social Engineering?

Janiesch: Völlig zutreffend, wobei dies in unterschiedlichen Formen erfolgt. So sind z. B. manipulierte E-Mails mit Schadprogrammen auf die jeweiligen Arbeits- und Interessengebiete zugeschnitten, um die Adressaten leichter zum Öffnen zu verleiten. Eine weitere Gefahr geht von manipulierten USB-Sticks oder Ähnlichem aus. Auch hier setzen die Angreifer auf den sorglosen Umgang mit fremder Hardware, über die Netzwerke infiziert und ausgespäht werden. Ein weiterer Punkt betrifft den eigenen Umgang mit Netzwerken wie Facebook etc. Hier sollte jeder Nutzer sensibel darauf achten, welche Daten er von sich preisgibt und dass Firmeninterna, sollten sie auch noch so unbedeutend scheinen, hier zur Veröffentlichung absolut nichts zu suchen haben.

Welche Unterstützung können private Sicherheitsunternehmen leisten?

Janiesch: Die Unterstützung basiert auf zwei Säulen. Zum einen geht es um internetspezifische Schutzmaßnahmen wie Firewalls und Verschlüsselungstechnologien. Zum anderen kommt klassischen Elementen der Unternehmenssicherheit inklusive der Beratung und Umsetzung durch den Dienstleister eine ganz zentrale Rolle zu.

Können Sie dies anhand von Beispielen konkretisieren?

Janiesch: Dies beginnt mit der Einrichtung von Zutrittskontrollsystemen, damit ungebetene Besucher, etwa als vermeintliche Lieferanten getarnt, keinen Zugriff auf PC oder sensible EDV-Bereiche bekommen. Zudem geht es um die Implementierung von

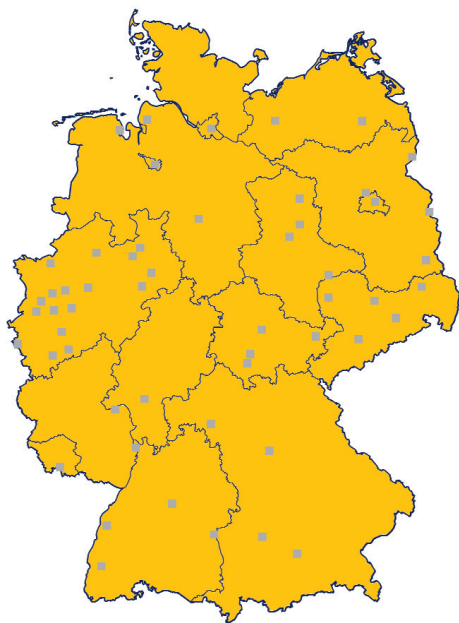
Richtlinien für die Internetnutzung am Arbeitsplatz, für den Umgang mit Passwörtern und Zugriffsberechtigungen etc. Besonders wichtig ist außerdem die Sensibilisierung der Mitarbeiter für die wachsenden Cybercrime-Gefahren. Hierbei ist u. a. der richtige Umgang mit E-Mails verdächtiger Absender zum Schutz vor Viren, Trojanern etc. gemeint oder die Gefahr der Infizierung mit Schadprogrammen beim Surfen auf unbekanntem Internetseiten.

Und was kann auf staatlicher Ebene weiter getan werden?

Janiesch: Die im Sommer erfolgte Eröffnung des nationalen Cyberabwehrzentrums, das als Informations- und Austauschplattform Angriffe bewertet und Empfehlungen für Institutionen und Unternehmen abgibt, war ein wichtiger Schritt. Diese Anstrengungen

müssen weiter verstärkt werden, sowohl national wie international. Bestandteil der Überlegungen zur Cybercrime-Bekämpfung ist auch das Thema Vorratsdatenspeicherung. Gleichzeitig kommt der intensiven Kooperation von Behörden und Wirtschaft eine zentrale Rolle zu – gerade mit Blick auf die Sicherheit kritischer Infrastrukturen wie Energie, Logistik und Telekommunikation. Auch an diesen Stellen können die Dienstleister unterstützen: zum einen durch ihre Kompetenzen beim Schutz kritischer Infrastrukturen; zum anderen durch die Entlastung der öffentlichen Hand, die so frei werdende Ressourcen u. a. für ihre Kernaufgaben der Kriminalitätsbekämpfung, Gefahrenabwehr und Vorbeugung vor Straftaten nutzen kann.

Das Interview führte Carsten Gronwald, Referent für Presse- und Öffentlichkeitsarbeit, KÖTTER GmbH & Co. KG Verwaltungsdienstleistungen.



KÖTTER Services in Deutschland

Aachen
Augsburg
Berlin
Bielefeld
Bitterfeld
Bonn
Bremen
Büren
Burg
Chemnitz
Cottbus
Dortmund
Dresden
Düsseldorf
Duisburg
Erfurt
Essen
Euskirchen

Frankfurt am Main
Frankfurt (Oder)
Freiburg
Gera
Gütersloh
Hamburg
Hannover
Hennigsdorf
Hoyerswerda
Ingelheim
Köln
Krefeld
Langen
Leipzig
Magdeburg
Mannheim
Mönchengladbach
München

Münster
Neubrandenburg
Nürnberg
Oberhof
Offenburg
Paderborn
Rhede
Riesa
Saarbrücken
Schwedt
Schwerin
Stendal
Stuttgart
Suhl
Ulm
Wilhelmshaven
Würzburg
Wuppertal



„Wir sind für Sie da.“

Wilhelm-Beckmann-Straße 7
45307 Essen

Hotline: +49 201 2788-388
Hotfax: +49 201 2788-488
E-Mail: info@koetter.de

Internet: www.koetter.de

Impressum:

Der **Sicherheitsbrief** wird herausgegeben von der Öffentlichkeitsarbeit der KÖTTER GmbH & Co. KG Verwaltungsdienstleistungen.
Tel.: +49 201 2788-126, Fax: +49 201 2788-178, E-Mail: carsten.gronwald@koetter.de
© Die Zeitschrift und alle darin enthaltenen Beiträge sind urheberrechtlich geschützt.
Die Mitgliedschaft in den aufgeführten Verbänden gilt für Einzelfirmen der KÖTTER Unternehmensgruppe. Bildmaterial: Fotolia LLC

