Zeitschrift: ASMZ : Sicherheit Schweiz : Allgemeine schweizerische Militärzeitschrift

Herausgeber: Schweizerische Offiziersgesellschaft

Band: 183 (2017)

Heft: 7

Artikel: Sicherheitsverbund Schweiz I : Cyber-Kriminalität im Fokus

Autor: Heim, Karl J.

DOI: https://doi.org/10.5169/seals-730665

Nutzungsbedingungen

Die ETH-Bibliothek ist die Anbieterin der digitalisierten Zeitschriften auf E-Periodica. Sie besitzt keine Urheberrechte an den Zeitschriften und ist nicht verantwortlich für deren Inhalte. Die Rechte liegen in der Regel bei den Herausgebern beziehungsweise den externen Rechteinhabern. Das Veröffentlichen von Bildern in Print- und Online-Publikationen sowie auf Social Media-Kanälen oder Webseiten ist nur mit vorheriger Genehmigung der Rechteinhaber erlaubt. Mehr erfahren

Conditions d'utilisation

L'ETH Library est le fournisseur des revues numérisées. Elle ne détient aucun droit d'auteur sur les revues et n'est pas responsable de leur contenu. En règle générale, les droits sont détenus par les éditeurs ou les détenteurs de droits externes. La reproduction d'images dans des publications imprimées ou en ligne ainsi que sur des canaux de médias sociaux ou des sites web n'est autorisée qu'avec l'accord préalable des détenteurs des droits. En savoir plus

Terms of use

The ETH Library is the provider of the digitised journals. It does not own any copyrights to the journals and is not responsible for their content. The rights usually lie with the publishers or the external rights holders. Publishing images in print and online publications, as well as on social media channels or websites, is only permitted with the prior consent of the rights holders. Find out more

Download PDF: 11.01.2026

ETH-Bibliothek Zürich, E-Periodica, https://www.e-periodica.ch

Sicherheitsverbund Schweiz I: Cyber-Kriminalität im Fokus

Wenig steigert aktuell das Sicherheitsbedürfnis stärker als cyber-kriminelle Aktivitäten. Daraus gewann der Sicherheitsverbund Schweiz (SVS) das Leitthema für seine dritte Konferenz. Alle Akteure mit sicherheitsrelevanter Verantwortung müssen sich den neuen Bedrohungsformen stellen, rasch reagieren und den Bereitschaftsgrad erhöhen.

Karl J. Heim

Schneller sein als die Täter in der Prävention dieser virulenter auftretenden, doch noch immer neuartigen Form von «White Collar»-Kriminalität? Dies funktioniert selten und höchstens unter grossem Aufwand, da es sich oft um ausgebuffte Experten-Verbrecher handelt, welche von der digitalen Tarnkappe profitieren. Nationale Grenzen sind in diesen Sphären ohnehin inexistent.

Nach bewährtem Muster wechselten in dieser dritten Konferenz hochkarätige Vorträge mit spannenden Podiumsdiskussionen ab, welche die Referenten einbezogen. Dabei kristallisierte sich heraus, dass dem Phänomen Cyber-Kriminalität auf Dauer nur durch ein mindestens ebenbürtiges Repertoire an Hacker-Know-how und vor allem durch unverzügliches Reagieren mit diversen Massnahmen beizukommen ist. Dabei sind Justiz und Überwachung auf Seiten des Staates ebenso sehr gefordert wie Innovationsfähigkeit der Unternehmen zur Früherkennung digitaler Angriffe.

Konferenzleiter André Duvillard, Delegierter für den SVS.

Kampf der Malware

Sei es das Lausanner Universitätsspital (kurz «CHUV» für «Centre hospitalier universitaire vaudois») oder die SBB oder andere grosse Institutionen primär aus dem öffentlichen Bereich: Die Gefahren der Cyber-Kriminalität lauern mittlerweile überall. Die öffentliche Verwaltung, aber auch kundenorientierte Dienstleister der Privatwirtschaft wie Krankenkassen exponieren sich besonders, weil ihre riesigen Mengen an Daten natürlicher Personen sehr attraktiv für verbrecherische Aktionen sind. Je mehr Vorgänge und Strukturen digitalisiert und vernetzt sind, desto stärker wachsen die Angriffsflächen. Damit halten die Schutzmassnahmen kaum Schritt.

Streit über Grenzen der Schweizer Zuständigkeit

Eine der grössten Gefahren von Cyber-Kriminalität geht für Bundesanwalt Michael Lauber vom «Phishing» aus, dem Ausspionieren von Zugriffsdaten vor allem von Kreditkarten mittels betrügerischer E-Mails, welchen infizierte Anhänge beigefügt sind. So wurden in einem Fall allein durch vier Marokkaner rund 100 000 Kreditkarten abgeschöpft, davon 3000 in der Schweiz. Mithin keine kleinen Fische, deren man selten oder nur mit grössten Schwierigkeiten habhaft werden kann. Die Bundesanwaltschaft erhob Anklage für sämtliche 100 000 geschädigte Kreditkarten-Inhaber, der Haupttäter hat gar mit den Behörden kooperiert.

Die spektakulären und mit grossem Aufwand gewonnenen Erkenntnisse hindern die Justiz nicht daran, den Ermittlungen der Bundesanwaltschaft einen Riegel zu schieben: Denn der Server und damit die Tatorte befinden sich in den USA. Direkte, also nicht auf dem Weg der Rechtshilfe betriebene Ermittlungen hält das Bundesstrafgericht für Einmischung in die inneren Angelegenheiten eines anderen Staates. Auf den Abschluss von Rechtshilfeverfahren solchen Umfanges wartet die ersuchende Behörde erfahrungsgemäss anderthalb Jahre. Dieses Ergebnis ist umso schwerer zu verstehen, als die Bundesanwaltschaft ihre Zuständigkeit entschieden bejaht; wie gemäss Artikel 6 StGB vorgesehen, gründe ihre Kompetenz auf einem Staatsvertrag, der «Cyber Crime Convention».

Die Kantone ziehen mit

Aus kantonaler Ankläger-Sicht verdeutlichte Beat Oppliger, Leitender Zürcher Oberstaatsanwalt, das Engagement gegen Cyber-Kriminalität. Dabei wurde deutlich, dass auch die Kantone am häufigsten mit dem Phishing-Phänomen konfrontiert sind, dem sie durch effiziente Prozesse und gute technische Ausrüstung zu begegnen trachten.

Oppliger berichtete von Erfahrungen, welche Zürich aus dem Betrieb seines Ende 2013 ins Leben gerufenen Kompetenzzentrums gewann, gemeinsam betrieben von Spezialisten der Justiz und der Polizei. Als Erfolgsfaktoren schälen sich heraus:

- Zeit – Geschwindigkeit des Verfahrens;
- Wissens- und Handlungskompetenz der eingesetzten Kräfte;
- Flexibilität in der Fallzuteilung;
- genügend Personalressourcen mit dem erforderlichen Know-how.

Zu den wesentlichen Rahmenbedingungen zählt Oppliger die örtliche Nähe der zusammenwirkenden Organisationen, das gemeinsame Rollenverständnis, auf einander abgestimmte Prozesse, die passende technische Ausrüstung, den Teamgeist und die Vernetzung national, international sowie mit dem privaten Sektor. Das leistet letztlich nur ein Kompetenzzentrum. ■

Oberstlt
Karl J. Heim
Think Tank HKA
lic. iur. Executive MBA FH
Rechtsdozent
4102 Binningen