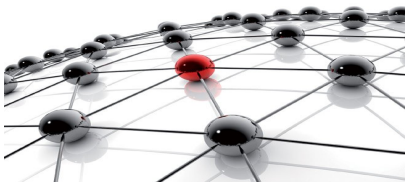
Im Einsatz – im Thema.
POLIZEI PRAXIS

KOMPETENZ IM CYBERRAUM



Aktuelles und umfassendes Know-how ist gerade im Cyber-Crime-Bereich ein elementarer Erfolgsfaktor, eine entsprechende Aus- und Weiterbildung trägt dazu entscheidend bei.

Cyber Security und Cyber Crime waren 2013 als Schlagworte sehr oft in den Medien präsent. In diesem Kontext wurden eine Unmenge an Zahlen und Statistiken produziert. So hat Kaspersky laut eigenen Angaben in 2013 täglich 315.000 neue Schadprogramme entdeckt, was einer Steigerung von über 57 Prozent gegenüber dem Vorjahr entspräche. Die Telekom gab an, dass über ihre Honeypots täglich bis zu 800.000 Hackerangriffe registriert worden sind. Laut Fraunhofer FKIE können mittlerweile Denial of Services -Angriffe unter Nutzung von Bot-Netzen (DDoS) mit einer Kapazität von 80 Gbit/s durchgeführt werden.

Dem einhergehend gab es zahlreiche Berichte zu Sicherheitsvorfällen bei bekannten Unternehmen und bei Behörden. Daneben erschienen auch Meldungen, welche auf den ersten Blick eine gewisse komische Note hatten. So hatten „gute Hacker“ entdeckt, dass man in die zentrale IT von Kirchen eindringen konnte und folglich zu beliebigen Zeiten die Kirchenglocken hätte läuten können.

Sicherheitsexperten haben herausgefunden, dass auch Schiffsüberwachungssysteme, welche die aktuellen Positionen von Schiffen weltweit darstellen, relativ leicht über das Internet von außen manipuliert werden können. Man könnte also quasi „Schiffe versenken“ spielen und diese, zumindest digital, verschwinden lassen. Letztlich zeigt dies alles sehr plakativ, dass unser tägliches Leben zunehmend „vernetzt“ ist. Viele Vorgänge sind ohne IT und Internet überhaupt nicht mehr möglich.

Datenfülle und Datenvielfalt

Der Smartphone-Trend spiegelt dabei deutlich den Wunsch nach ständiger Verfügbarkeit von Daten wieder. Geht es nach der Industrie, dann werden wir in 2014 viele Menschen auf den Straßen antreffen, welche mit Datenbrillen herumlaufen und Informationen auf Abruf buchstäblich vor Augen geführt bekommen.

Als Begleiterscheinung der schnell ansteigenden Datenfülle und -vielfalt liegen schon heute viele Informationen nur mehr in digitaler Form vor, existieren also alleinig im Cyberraum!

Diese digitale Welt mit ihren zahllosen Möglichkeiten eröffnet auch für Kriminelle ein vielversprechendes Betätigungsfeld und eine attraktive Alternative zur althergebrachten analogen Kriminalität: Ein Diebstahl im Cyberraum ist einfacher, risikoärmer und effektiver als ein konventioneller Banküberfall. Ein Cyber-Angriff kann im Prinzip von jedem Ort der Welt aus erfolgen, die Auswirkungen machen sich ganz woanders bemerkbar. Dabei werden Prävention und Strafverfolgung durch die hohe technologische Komplexität und die schnelle Fortentwicklung der Angriffsmittel und -methoden erschwert. Hinzu kommt, dass durch die einfache Zugänglichkeit von Hacking-Tools und entsprechender Support-Leistungen der Hersteller mittlerweile auch Nicht-Experten in der Lage sind, wirkungsvolle Cyberangriffe durchzuführen.

Die Polizeiliche Kriminalstatistik 2012 sprach von einem Anstieg der Straftaten im Bereich Computerkriminalität unter Nutzung moderner Informations- und Kommunikationsmittel um 8% auf 63.959 Straftaten bei einer Aufklärungsquote von 26,5%. Die deutlichste Steigerung war hier im Bereich Datenveränderung und Computersabotage mit 133,8 Prozent zu verzeichnen.

Auch Polizei betroffen

Diese letzte Zahl bestätigt, dass es nicht immer darum geht, Informationen zu entwenden. Genauso kann es Absicht sein, die IT lahmzulegen, um Geschäftsprozesse bei einem Konkurrenten zu sabotieren, oder Daten zu verändern, um den guten Ruf einer Institution zu schädigen. Großes Aufsehen gab es, als es Kriminellen im August 2013 gelang, die Washington Post zu hacken und Inhalte auf deren Webseiten zu verändern. Aber auch Internetportale der Polizei in Deutschland waren bereits Opfer von Cyberangriffen.

Dies zeigt, dass die Polizei gleich in mehrerlei Hinsicht betroffen ist: Zum einen obliegt es natürlich der Polizei, bei entsprechenden Vorfällen ermittelnd tätig zu werden. Darüber hinaus erwartet die Gesellschaft bei der Polizei eine Anlaufstelle vorzufinden, welche kompetent Ratschläge in allen Cyber Crime-Fragen erteilen kann. Nicht zuletzt können aber polizeiliche Stellen aufgrund ihrer wichtigen Funktion für die Gesellschaft und der hochsensiblen Daten, welche hier verarbeitet werden, auch selbst ins Fadenkreuz von Angreifern rücken.
Dies alles ist für Fachleute nicht neu, macht aber die Bedeutung deutlich, welche eine entsprechende Aus- und Fortbildung gerade im polizeilichen Bereich hat:

Eine gute Qualifizierung ist vor allem für das im Cyber Crime-Bereich tätige Personal elementar. Wesentliches Erfolgskriterium ist hier ein umfassendes Know-how hinsichtlich der zahlreichen technologischen Möglichkeiten und Methoden zur Ausführung von Cyber-Angriffen, der entsprechenden Schutz- und Gegenmaßnahmen und der forensischen Mittel und Verfahren. In Anbetracht der rasanten Veränderungen im Cyberraum ist dieses Wissen jedoch schnell veraltet und muss deshalb permanent aktualisiert werden.

Um parallel organisationsintern ein effizientes Schutzniveau zu gewährleisten, sollten alle Mitarbeiter einer Polizeibehörde eine gewisse Mindestkompetenz und Sensibilität hinsichtlich der Thematik IT-Sicherheit aufweisen.

Qualifikationsbedarf

Diesen Qualifikationsbedarf hinsichtlich Cyber-Sicherheit hat die Cyber Akademie (CAk) im Fokus. Sie wurde als gemeinsame Initiative des Behörden Spiegel und der Gewerkschaft der Polizei (GdP) ins Leben gerufen. Die CAk-Fortbildungen adressieren die spezifischen Anforderungen von öffentlicher Verwaltung und Sicherheitsbehörden. Das Seminarangebot ist dabei als Ergänzung zu den Ausbildungsprogrammen der öffentlichen Schulungseinrichtungen auf Bundes- und Landesebene angedacht.

Als Dozenten treten in den Seminaren der CAk ausschließlich Experten auf, welche hauptberuflich „an der Front“ agieren: Sie sind beispielsweise als IT-Sicherheitsberater bei Behörden und Unternehmen tätig oder führen Entwicklungs- und Forschungsprojekte zu IT-Sicherheitsthemen durch. Auf diese Weise kann sichergestellt werden, dass in den CAk-Seminaren der aktuelle Stand von Technologien, Methoden und Trends berücksichtigt wird.

Seminarangebote

Cyber-Sicherheit ist eine Herausforderung, welche nur durch eine Organisation als Ganzes bewältigt werden kann. Die CAk bietet deshalb für alle Ebenen, vom Mitarbeiter bis zur Behördenleitung, entsprechende Seminare oder auch Sensibilisierungsschulungen an.
Umfängliches Grundlagenwissen vermitteln die Ausbildungen zum IT-Sicherheits- oder Datenschutzbeauftragten mit TÜV-Personenzertifizierung. Diese Schulungen werden in Kooperation mit PersCert TÜV des TÜV Rheinland durchgeführt.

In den Fortbildungsseminaren greift die CAk alle Aspekte und Trends auf, welche für IT-Sicherheit und Datenschutz von Bedeutung sind. Die Bandbreite reicht dabei von strategischen IuK-Grundlagen und -Entwicklungen über Notfallmanagement bis hin zu eher technisch-orientierten Themen, wie Mobile Device Security, aktuelle Hacking- Methoden und Webanwendungssicherheit. Vor allem letztere Kategorie von Fortbildungen erfährt sehr große Resonanz aus dem polizeilichen Bereich. In dieser Seminarsparte werden demnächst auch Methoden und Mittel zur Früherkennung von Cyberangriffen und die IT-Forensik thematisiert.
Ralf Kaschow, Cyber Akademie

Alle Artikel dieser Kategorie

Folgen Sie uns!