Anwalt aktuell **11.04.2017**
Erscheinungsland: Österreich | Auflage: 30.000 | Reichweite: k.A. (k.A.) | Artikelumfang: 73.352 mm² Seite: 12 1/2

Thema: Mathias Preuschl
Autor: k.A.

CYBERDELIKTE

Cyberkriminalität 2.0
Daten sind die neue Währung

Attacken auf die Internetseiten politischer Gegner, Datenklau bei Kreditkartenunternehmen oder Erpressung eines Hotels durch Kapern der Buchungssoftware. Ein aufmerksamer Blick in die Medien beweist; das klassische Eigentumsdelikt wird immer mehr zum Refugium für den dummen Kriminellen, der etwas gewieftere Verbrecher begeht seine Taten in und mit dem Internet.

DR. MATHIAS PREUSCHL
Partner von PHH Rechtsanwälte ist Spezialist für Wirtschafts- und Unternehmensstrafrecht und Datenschutz.

Die Ursachen für diese Entwicklung sind zum einen die Möglichkeit – war Hacken jahrelang die Domäne einiger weniger Nerds mit sozialen und Hauptproblemen so ist es jetzt auf dem besten Weg zum Breitensport. Man benötigt keine Programmierkenntnisse; Viren und Würmer können entweder in einem benutzerfreundlichen Bausteinprogramm selbst zusammengestellt werden oder einfach von der Stange erworben werden. Zum anderen die Risiko-Nutzen Relation für den Täter: Es wird der klassische Bankraub aufgrund moderner Überwachungs- und Aufklärungsmethoden nicht nur immer riskanter, sondern wird auch die erzielbare Beute aufgrund der geringeren Bargeldbestände in den Bankfilialen immer magerer. Demgegenüber steht die Komfortabilität des Cyberangriffs von der Couch aus und die Tatsache, dass je nach Delikt hier eine gewaltige Bandbreite an „Erträgen" besteht. Auch können Cyberdelikte von irgendeinem Punkt der Erde begangen werden, solange dort nur eine gute Internetverbindung besteht: Besonders entgegenkommend ist für den Täter, wenn dieser Punkt sich in einem Staat mit schwachen rechtsstaatlichen Strukturen befindet.

Daten sind die neue Währung

Der Klassiker unter den Cyberdelikten ist – wie auch in der analogen Welt – der Diebstahl. Egal ob Kreditkarten- oder Datingplattformdaten, gestohlen wird alles was, nicht niet- und nagelfest ist, und das ist in der digitalen Welt nicht wenig. Keine Woche vergeht, in der nicht der Verlust von abertausenden Daten eingestanden wird. Die Verwertung ist denkbar einfach: entweder direkt, wie bei Kreditkartendaten durch schlichtes Benutzen oder etwas komplizierter, wie bei Datingplattformdaten oder sehr privaten digitalen Fotos, durch Erpressung. Letztere ist auch die nunmehr rasant steigende Form der Cyberkriminalität. Daten werden nicht mehr gestohlen, sondern mittels sogenannter Ransomware verschlüsselt. Dem Opfer wird dann mitgeteilt, dass sie nach Zahlung des Lösegeldes kannter Absender nicht öffnet bzw. anklickt, so hat man schon die meisten Angriffspunkte für Cyberkriminelle ausgeschaltet.

Thema: Mathias Preuschl

Autor: k.A.

wieder entschlüsselt werden. Das Beutespektrum reicht hier von einigen hundert Euro für private Daten bis zu einigen hunderttausend Euro für die Daten eines ganzen Krankenhauses. Zuletzt sei auch nicht die (Industrie-) Spionage bzw. Sabotage durch Hackerangriffe erwähnt. Hier werden nicht nur Schäden in Milliardenhöhe angerichtet, sondern stellt dies auch den Bereich der Cyberkriminalität dar in welchem sich Kriminelle das Feld mit Geheimdiensten und Terroristen teilen.

Gegenstrategie Vorsicht

Wie auch in der analogen Kriminalitätsbekämpfung ist Vorbeugung alles. Eine funktionierende und aktuelle Firewall, ein Server auf dem neuesten Stand und Passworte, die aus etwas mehr als den eigenen Initialen samt Geburtsdatum bestehen, schrecken schon einen Großteil der Täter ab. Auch eine Sensibilisierung der Mitarbeiter im Unternehmen ist nötig, weder ist ein Passwort auf einen Zettel aufzuschreiben, noch ist es dem freundlichen IT Techniker, der nach Dienstschluss zu Hause anruft mitzuteilen. Wenn man zudem noch die Absendeadresse von Emails etwas genauer prüft und insbesondere Anhänge von bzw. Links in Emails unbe-

Was aber tun, wenn ein Angriff dennoch passiert ist?

Wesentlich ist es einen Plan zu haben, bevor der Ernstfall eintritt; dieser muss klare Anweisungen enthalten wie z.B. Isolierung der betroffenen Rechner, Zuständigkeiten der internen/ externen IT Techniker und Verhaltensregel für alle Mitarbeiter. Ist die unmittelbare Gefahr einmal gebannt, so gilt es den Schaden zu minimieren und die Täter zu verfolgen. Hier ist eine schnelle Kontaktaufnahme mit den Strafverfolgungsbehörden nötig um nicht nur allfällige Geldflüsse noch zu stoppen, was in der Praxis zumindest teilweise gelingt, sondern ist eine umfassende Information der Exekutive auch nötig, um gleichartige Taten zu verhindern. Gerade die falsche Scham vieler Opfer ist im Bereich der Cyberkriminalität die größte Hürde für die Verfolgung der Täter aber auch die Prävention. Vernetzungsprojekte in einigen Branchen, durch die Informationen rasch ausgetauscht werden, haben dort schon zu einem signifikanten Absinken der erfolgreichen Angriffe geführt.

Dr. Mathias Preuschl, Partner von PHH Rechtsanwälte ist Spezialist für Wirtschafts- und Unternehmensstrafrecht und Datenschutz.