Forum 4

Sicherheit in der digitalen Welt – Cyber Security in Recht und Praxis

Arno Bernhardt, Airbus Defence and Space GmbH

Die aktuelle Bedrohungslage ist hoch: Cyberkriminalität ist unter den Top 10 der größten Geschäftsrisiken. Betrachtet man im Internet die Seite https://cybermap.kaspersky.com, so findet man dort eine Cybermap, auf der man die von der Software des Cybersecurity-Unternehmens Kaspersky abgewehrte Cyberattacken in Echtzeit sehen kann. Deutschland steht meistens unter den Top 3 der am meisten angegriffenen Länder. Die Angreifer werden auch immer professioneller – kein Wunder, sind (Stand August 2016) ja 560 Millionen Schadprogrammvarianten bekannt. Auch die zunehmende Vernetzung durch die fortschreitende Digitalisierung (wie z. B durch das Internet der Dinge) sowie die steigende Komplexität von IT-Systemen vereinfachen die Lage nicht.

Der Referent Arno Bernhardt ist Rechtsanwalt und war zunächst für eine renommierte Kanzlei in Mailand tätig. Seit Mitte 2002 ist er als Unternehmensjurist bei Airbus beschäftigt. Schwerpunkte seiner Tätigkeit sind dort der gewerbliche Rechtsschutz und das IT-Recht. Er ist u. a. für die juristische Betreuung der deutschen Gesellschaft von Airbus Cybersecurity verantwortlich.

Um einen Einblick in das Thema zu bekommen, sind zuerst einige Begrifflichkeiten zu klären, anschließend werden verschiedene Cyber-Angriffsarten erklärt. Nach einer Typologie der Angreifer werden einige Beispiele genannt, abschließend gibt es einen kurzen Überblick über die aktuelle Gesetzeslage.

Begrifflichkeiten

Unter den Schutzgütern der IT-Sicherheit versteht man die **Verfügbarkeit** („Komme ich an meine Daten?“), die **Integrität** („Sind meine Daten unversehrt und vollständig?“), die **Vertraulichkeit** („Sind meine vertraulichen Daten bei mir und nicht anderswo?“) und die **Authentizität** („Kann ich Daten sicher zuordnen, d. h. ist z. B. die E-Mail tatsächlich von demjenigen, dessen Namen in der Absenderzeile steht?“).

Unter dem Cyberraum versteht man im allgemeinen das Internet, Cybersecurity ist demnach die Sicherheit im Internet, ein Cyber-Angriff greift dieses Internet an. IT-Sicherheit ist wiederum mehr als Cybersecurity, zu dieser kommen noch die physische Sicherheit der Computeranlagen (Zugangsbeschränkungen, Bewachung u. ä.) sowie IT-Sicherheitsprozesse hinzu. Unter IT-Sicherheitsprozessen versteht man standardisierte Prozesse, welche den genauen Ablauf vor (Prävention), nach oder während eines Cyberangriffs vorgeben, so dass nicht erst Zeit verloren geht, um Entscheidungen zu treffen oder anderweitig nachzufragen.

Angriffsarten

Wird man mit **Ransomware** (Ransom = engl. Lösegeld) angegriffen, so werden meist alle Daten auf dem Computer verschlüsselt und der Angreifer fordert ein Lösegeld in Form von Bitcoins, um die Daten wieder zu entschlüsseln. Laut einer Auswertung des Softwareanbieters Citrix halten mittlerweile knapp zwei Drittel der Unternehmen Bitcoins für solche Erpressungsfälle bereit.

Social Engineering nennt man zwischenmenschliche Beeinflussungen mit dem Ziel, bei Personen bestimmte Verhaltensweisen hervorzurufen. Das kann einerseits der zufällig auf dem Firmenparkplatz liegende USB-Stick sein, der dann, sobald er unvorsichtigerweise an den Computer angeschlossen wurde, das Schadprogramm aufspielt. Andererseits funktioniert das aber auch mit Geburtstagskarten (Geburtstagsdatum erhält man ja über Facebook, XING, LinkedIn und Co), welche dann von einer Fake-Email-Adresse (mit dem Namen eines Bekannten von ebenden genannten Plattformen versehen) versandt werden. Auch hier löst der Klick den Download des oder direkt das Schadprogramm aus.

Advanced Persistent Threat (ATP) ist eine der perfiden Angriffsmethoden. Hierbei verschaffen sich Angreifer sehr langsam immer weiter Zutritt in das jeweilige Netzwerk bzw. Computersystem. Häufig werden diese komplexen, zielgerichteten und effektiven Angriffe erst Monate nach dem ersten Eindringen bemerkt. Diese Art des Cyber-Angriffs ist sehr zeitintensiv und aufwändig, deshalb wird er meist von sehr professionellen Angreifern durchgeführt. Ziel ist es, über einen längeren Zeitraum immer wieder Informationen abzuschöpfen, unentdeckt zu bleiben und weiter vorzudringen.

Der Angriff durch **Spam** klingt zwar zuerst weniger bedrohlich, doch auch eine Spam-Flut kann ein Unternehmen in der Ausführung seiner Geschäfte behindern und zu Kosten führen.

Botnetze bezeichnen eine Sammlung kompromittierter PCs, die ein Angreifer aus der Ferne kontrollieren kann. Diese werden normalerweise von einem einzelnen Angreifer oder einer Gruppe aufgebaut. Dabei nutzen sie ein Schadprogramm, um möglichst viele Computer zu infizieren. Mittlerweile kann man sich aber Rechnerleistung durch Botnetze auch im Darknet kaufen. Botnetze werden für **Distributed Denial of Service** (DDoS) Angriffe benötigt, bei welchen diese Rechner zum Angriffswerkzeug werden und auf Kommando des Hackers ein bestimmtes Ziel, zum Beispiel einen Web-Server, mit gefälschten Anfragen bombardieren. Dieser wird dadurch dann außer Gefecht gesetzt.

Gegen die Angriffsart „**Drive by Exploits**“ ist man meist machtlos. Hier werden beim Betrachten einer Webseite durch manipulierte Werbebanner ohne weitere Nutzerinteraktion Schwachstellen im Browser, in Browser-Plugins oder im Betriebssystem ausgenutzt, um Schadsoftware unbemerkt auf dem PC zu installieren.

Beim **Identitätsdiebstahl** werden, wie der Name schon sagt, Identitätsprofile gestohlen, um diese dann weiterzuverkaufen oder anderweitig, zum Beispiel beim Social Engineering einzusetzen.

Mehrstufige Angriffe werden angewendet, wenn man nicht direkt sein Zielobjekt angreift. So sind z. B. die Sicherheitsvorkehrungen großer Unternehmen häufig schwer zu knacken. Um dennoch in das System zu kommen, greift man also den weniger gut geschützten Zulieferer an. Ist man in dessen System, kann sich das Schadprogramm zum nächsten Zulieferer weiterverbreiten und so letztendlich in die Firma eindringen, da man z. B. E-Mails oder Downloads von bekannten Adressen seiner Zulieferer grundsätzlich vertraut.

Nicht vergessen darf man auch **Hardware Manipulationen**, die mit den üblichen Maßnahmen (Firewall oder Virenscanner) nicht zu entdecken sind.

Angreifer-Typologie

Wer aber macht so etwas? Hier gibt es einerseits die Cyber-Aktivisten, die Webseiten hacken, um ähnlich zu ihrem analogen Pendant ihre Botschaft in die Welt zu streuen. Daneben gibt es aber auch hochorganisierte Banden, die sogenannten Cyber-Kriminellen. Weitere selbsterklärende Typen sind Nachrichtendienste, Unternehmen oder auch staatliche Akteure. Hier stehen jeweils wirtschaftliche oder politische Interessen im Vordergrund. Cyber-Terroristen hingegen wollen vor allem größtmöglichen Schaden anrichten, ihnen geht es nicht um die eigene Bereicherung wie den Cyber-Kriminellen. Hobbyisten oder sog. Skript Kiddies hingegen wollen einfach einmal ausprobieren, wie weit man gehen kann. Das dies sehr leichtsinnig sein kann, erkennt man an der Rechtslage, nach der bei Cyberangriffen zum Teil sehr hohe Schadensersatzforderungen den geschädigten Unternehmen zugesprochen werden können.

Eine weitere Gruppe, die sich auf Cyber-Angriffe spezialisiert hat, sind natürlich die IT-Sicherheitsforscher, die hier aber nur der Form halber genannt werden, da sie keinerlei Gemeinsamkeiten mit den vorher genannten Personenkreisen haben.

„Best Practice"-Beispiele

Herr Bernhardt nennt einige bekanntgewordene Fälle, bei denen Cyberangriffe bemerkenswert gut gelungen sind. Die genauen Berichte dazu kann man gut im Internet nachrecherchieren, hier soll eine Aufzählung reichen:

- Der Schweizer Rüstungskonzern Ruag wurde Opfer eines professionellen Datendiebstahls.
- Der weltweite Angriff mit der Ransomware WannaCry legte u. a. Krankenhäuser in England lahm.
- Zwei Hackern gelang es, sich in die Software eines Jeeps einzuhacken und die Kontrolle über den Wagen zu übernehmen.
- Das Programm CCleaner wurde gehackt, bei einem Update wurde vom User dann automatisch auch ein Virus heruntergeladen.
- Der deutsche Paktdienst wurde auch gehackt. Nachzulesen ist das im Online verfügbaren Artikel „Wie aus einem Nerd ein Hacker wurde" der Wirtschaftswoche.

Rechtliche Aspekte

Die grundlegende Frage, die sich der Gesetzgeber hier stellen musste ist: Wo fängt man bei der Gesetzgebung an, wenn man eine signifikante Verbesserung der IT-Sicherheit in Deutschland erreichen möchte? Das IT-Sicherheitsgesetz (IT-SiG), ein Artikelgesetz, das im wesentlichen Änderungen im Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSIG), aber auch in anderen Gesetzen wie z. B. dem Telemediengesetz (TMG) vorsieht, war hier der erste Schritt.

Besondere Bedeutung haben hierbei Infrastrukturen, die für das Funktionieren des Gemeinwesens zentral sind, sogenannte „Kritische Infrastrukturen" (kurz: KRITIS). Diese werden im § 2 Abs. 10 BSIG definiert als „Einrichtungen, Anlagen oder Teile davon, die den Sektoren Energie, Informationstechnik und Telekommunikation, Transport und Verkehr, Gesundheit, Wasser, Ernährung sowie Finanz- und Versicherungswesen angehören und von hoher Bedeutung für das Funktionieren des Gemeinwesens sind, weil durch ihren Ausfall oder ihre Beeinträchtigung erhebliche Versorgungsengpässe oder Gefährdungen für die öffentliche Sicherheit eintreten würden."

Als aktuelle Entwicklung wurde auch das Gesetz zur Umsetzung der europäischen Richtlinie zur Gewährleistung einer hohen Netzwerk- und Informationssicherheit (NIS-Richtlinie) genannt. Diese Richtlinie definiert Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der europäischen Union.

Auch im Strafrecht findet man viele Anknüpfungspunkte, genannt wurden hier die §§ 202a ff., 263a, 269, 202a f. StGB. Als Beispiel nannte Herr Bernhardt für die §§ 202a f. StGB den Fall „Handy-Lauscher vor Gericht: Wenn Liebling mitliest“, nachzulesen Online unter sueddeutsche.de, für § 263a StGB (Computerbetrug) den Fall des BGH mit der Nummer BGH 4 StR 194/16 (ebenfalls Online verfügbar).

Zum Abschluss wurden auch noch die haftungsrechtlichen Perspektiven aufgezeigt. Herr Bernhardt verwies hier auf die möglichen sehr hohen Schadensersatzforderungen nach § 823 BGB, die auf einen Hacker zukommen können, falls er ein großes Unternehmen über einen bestimmten Zeitraum lahmlegt.

Fazit

Abschließend lässt sich wohl sagen, dass man in diesem Forum einen kleinen Einblick in die sehr weite Welt der IT-Sicherheit werfen konnte. Vielleicht findet ja auch die eine oder andere Wirtschaft-und-Recht-Lehrkraft außerhalb des WSG-Ws und des Faches Wirtschaftsinformatik die Zeit, in einigen Stunden dieses wichtige Thema zu behandeln und den Schülerinnen und Schüler einen Einblick zu bieten.

Ein herzlicher Dank hier nochmals an Herrn Bernhardt für ein gelungenes, informatives, unterhaltsames und auch sehr lehrreiches Forum!

Tobias Tyll