Cybercrime und die Bedrohungen für die Wirtschaft (Teil 1)

Von ORR & Ass. jur. Frank Grantz, Altenholz

1 Einleitung

Bereits im Jahre 2014 führte der damalige FBI-Direktor James Comey aus: *„There are two types of American companies: those that have been hacked and those that don't know it yet."*[2]

Diese Aussage ist heute noch gültig und trifft sicherlich auch für die deutschen Wirtschaftsunternehmen zu. Ausweislich einer Studie von BITKOM[3] aus dem Jahre 2018 gaben z.B. 68% der befragten Industrieunternehmen an, Opfer von Cyberangriffen geworden zu sein, 19% gaben an, vermutlich betroffen zu sein.[4] Dazu gesellt sich eine hohe Dunkelziffer[5] und die Aussage von Strafverfolgungsbehörden, dass Cybercrimedelikte weiterhin ansteigen.[6] Insgesamt sind der deutschen Wirtschaft in den letzten 2 Jahren ca. 43,4 Mrd. Euro an Schäden durch Cyberangriffe entstanden.[7]

Dabei gibt es auch keine festgelegten Kostenarten, die tatsächlich unter diesen Schadensbegriff zu fassen sind, so dass die oben genannte Zahlen sicherlich nur als Anhalt dienen können. Denn gerade auch zusätzliche Personalkosten für die Störungsbeseitigung und vor allem die schwer zu erfassenden[8] Image- und Reputationsschäden bilden einen bedeutenden Faktor für ein wirtschaftlich ausgerichtetes Unternehmen; so sollen bspw. alleine 8,8 Mrd. Euro des gesamtwirtschaftlichen Schadens auf Image- und Reputationsschäden zurückzuführen sein.[9]

Die offene Struktur, die technischen Möglichkeiten und die Anonymität sind regelmäßig Ursachen dafür, dass das Internet als Angriffsplattform missbraucht wird. Aufgrund der mit der digitalen Vernetzung (Industrie 4.0[10], Internet of Things, Smart Cities) steigenden Komplexität der Systeme kommen altbekannte, konventionelle Sicherheitsmechanismen schnell an ihre Grenzen und vermögen es nicht, Zuverlässigkeit und Beherrschbarkeit in gewohntem Maße zu gewährleisten. Hinzu kommen weitere Angriffspunkte für Hacker, z.B. durch die Nutzung betrieblicher Smartphones oder der Nutzung von Clouds.

2 Cybercrime und IUK

Der internationale Begriff *„Cybercrime"* lässt sich aus juristischer Perspektive nicht eins zu eins ins Deutsche übertragen. Das BKA definiert in der jährlichen Veröffentlichung *„Cybercrime – Bundeslagebild"* unter diesem Schlagwort die Straftaten, die sich gegen das Internet, Datennetze, informationstechnische Systeme oder deren Daten richten (Cybercrime i.e.S.) oder die mittels dieser Informationstechnik begangen werden.[11] Des Weiteren werden auch Bezeichnungen wie EDV, Internetkriminalität, IUK oder Computerkriminalität verwendet, deren Ausprägungen sich regelmäßig durch neue Formen IT-basierter Angriffe fortentwickeln. Von Seiten der KPMG[12] wird zudem der Terminus *„ecrime"* definiert, und zwar als die Ausführung von

wirtschaftskriminellen Handlungen unter Einsatz von Informations- und Kommunikationstechnologien zum Schaden einer Einzelperson, eines Unternehmens oder einer Behörde.

3 Ausprägungen und gängige Angriffsmöglichkeiten

Als Angriffsmethoden und -mittel aus dem Bereich des Cybercrime werden regelmäßig ähnliche Modalitäten verwendet. Der BSI Lagebericht 2018[13] spricht im Wesentlichen von *„DDoS, Botnet und APT-Angriffen“*, von sog. *„drive by exploids“, „Spear Phishing“,* Infektionen mit Schadsoftware (Keylogger, Ransom, Trojaner oder Rootkits), aber auch das Vorgehen via Spammails und dem oft damit verbunden Social Engineering muss bedacht werden. Darüber hinaus gibt es Grundvoraussetzungen, bei deren Nichtbeachtung Schwachstellen entstehen, die dann gezielt als Einfallstor für Cyberangriffe genutzt werden können.

3.1 Allgemeine Schwachstellen

Aufgrund der umfassenden digitalen Möglichkeiten und vernetzten Anlagen ist das Wissen über diese Funktionsweise der Gesamtanlage mit kaum mehr überschaubaren Systemen und Anwenderprogrammen nur bei wenigen Fachleuten und Experten vorhanden. Für gewöhnliche Nutzer sind Fehler in eingesetzten Programmen nur erkennbar, falls sie offen am Bildschirm sichtbar sind oder zu einem unrichtigen Ergebnis führen. Die Kontrollmöglichkeiten der Nutzer bleiben damit beschränkt.[14]Lösungen sind zwar verfügbar, entsprechen jedoch häufig nicht den Anforderungen der Anwender an Komfort, Intuitivität und Bedienbarkeit.[15] Dieses stellt naturgemäß ein Risiko dar. Weitere Schwachstellen sind insbesondere veraltete Software und sog. *„ungepatchte*[16]“ Systeme. Vielfach werden selbst die bereits in der Software integrierten und einzustellenden Autoupdate Funktionen nicht genutzt. Auch das Nutzen veralteter Versionen von Betriebssystemen, die nicht mehr mit Patches unterstützt werden, stellt ein allgemeines Risiko und damit eine weitere Schwachstelle dar. Ein weiterer Problembereich sind die in Unternehmen vielfach genutzten mobilen Endgeräte. Sie stellen ein lohnendes Angriffsziel dar, da sie üblicherweise das komplette digitale (Arbeits-)Leben des Besitzers wiederspiegeln. Neben Gefahren durch Verlust und Diebstahl gibt es dabei besondere Herausforderungen bezüglich der IT Sicherheit auf dem Betriebssystem, dessen Aktualisierung und der installierten Apps. Um den jederzeitigen Zugriff auf Daten zu ermöglichen, werden zudem sog. eCloud[17]- Lösungen angeboten, die ebenfalls gerne zum Ziel von Hackerangriffen werden. Schließlich führt auch eine unzureichende Absicherung industrieller Steuersysteme zu einer besonderen Schwachstelle im Betrieb, insbesondere wenn durch die Entwicklung im Bereich der Industrie 4.0 die erweiterte Vernetzung dieser industriellen Steuerungssysteme über die internen Netze eines Unternehmens erfolgt ist.

IT-Labor einer Cybercrime-Dienststelle.

3.2 APT-Angriff (Advanced Persistent Threats)

Bei den APT handelt es sich um zielgerichtete Cyberangriffe auf spezifisch ausgewählte Institutionen und Einrichtungen, bei denen sich ein Angreifer persistenten Zugriff zu einem Opfernetzwerk verschafft und diesen in der Folge auf weitere Systeme ausweitet.[18] Angriffe verlaufen dabei häufig zunächst über wenig technikaffine Zielpersonen im Unternehmen, z.B. mittels dem Social Engineering. Die Erstinfektion erfolgt bspw. durch den Eingang einer E-Mail mit präpariertem Dokumentenanhang. Eine

weitere Möglichkeit besteht durch die sog. *„Watering Hole“* Angriffe. Dabei wird zunächst eine von der Zielperson häufig genutzte Webseite kompromittiert. Besucht die Zielpersonen dann diese Website, wird der Rechner mittels eines Drive by Exploits[19] mit einem Schadprogramm infiziert oder dem Opfer wird alternativ eine E-Mail mit dem Link auf eine präparierte Seite zugeschickt. Zugenommen hat in der initialen Phase der Angriffe auch die Verbindung von Installer- und Update-Hijacking.[20] Dabei werden auf Webseiten oder Update-Servern von Softwareherstellern Installationsarchive mit einem Schadcode versehen. Wenn die Nutzer dann die Programme herunterladen und installieren wird dadurch auch ein eingeschleustes Schadprogramm ausgeführt, das wiederum weitere Module nachladen kann.

Ebenso ist im aktuellen Trend das Spear Phishing gegen spezielle Personen erfolgreich, wo eine Email suggeriert von einer vertrauenswürdigen Quelle zu stammen und den Benutzer auf eine gefälschte Website lockt.

3.3 DDoS Angriffe

Eine weitere Angriffsmöglichkeit stellt der Denial-of-Service Angriff dar, der sich gezielt gegen die Verfügbarkeit von Diensten, Webseiten, einzelnen Systemen oder ganzen Netzen richtet. Bei einem solchen Procedere führen Angreifer die Nichtverfügbarkeit eines Dienstes oder Servers gezielt herbei. Sie infizieren dafür einen oder mehrere Rechner mit Schadsoftware und missbrauchen diese infizierten Rechnernetze, auch Botnetze genannt, ferngesteuert für ihre Attacken. Angegriffene Server ohne entsprechenden DDos Schutz sind mit den dann unzähligen Anfragen überfordert, ihre Internetleitung ist überlastet: Websites bauen sich nur noch stark verlangsamt auf oder sind überhaupt nicht mehr verfügbar. Das Ziel solcher Attacken ist vornehmlich das Herbeiführen von wirtschaftlichen Schäden der betroffenen Unternehmen, denn wenige Minuten offline kosten diesen schon einmal mehrere 1000 Euro.[21]

Bildrechte: Alexander Hahn und Redaktion.

(Fortsetzung folgt)

Anmerkungen

1. Oberregierungsrat Ass. jur. Frank Grantz ist hauptamtlicher Dozent im Fachbereich Polizei der FHVD Schleswig-Holstein.
2. www.independent.co.uk/news/business/news/fbis-james-comey-accuses-china-of-hacking-into-every-major-american-company-9777587.html=[130]%25.
3. Der Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V. (BITKOM) ist der Branchenverband der deutschen Informations- und Telekommunikationsbranche.
4. www.bitkom.org/Bitkom/Publikationen/Wirtschaftsschutzstudie-2018.html, S. 14.
5. www.bitkom.org/Bitkom/Publikationen/Wirtschaftsschutzstudie-2018.html, S. 5.
6. www.bka.de/SharedDocs/Downloads/DE/UnsereAufgaben/Deliktsbereiche/InternetKriminalitaet/handlungsempfehlungenWirtschaft.html,S.3f.
7. www.bitkom.org/Bitkom/Publikationen/Wirtschaftsschutzstudie-2018.html, S. 25.
8. Vgl. LG Köln, Urt. v. 28.7.2017, - 118 KLs 4/17 – juris Nr. 27ff.
9. www.bitkom.org/Bitkom/Publikationen/Wirtschaftsschutzstudie-2018.html, S. 25.
10. Industrie 4.0 (vierte industrielle Revolution) bezeichnet die intelligente Vernetzung von Maschinen und Abläufen in der Industrie mit Hilfe von Informations- und Kommunikationstechnologie. Übergeordnetes Ziel der Plattform Industrie 4.0 ist es, die internationale Spitzenposition Deutschlands in der produzierenden Industrie zu sichern und auszubauen.
11. www.bka.de/DE/AktuelleInformationen/StatistikenLagebilder/Lagebilder/Cybercrime/cybercrime_node.html, S. 4.
12. home.kpmg/de/de/home/themen/2017/04/ecrime-studie.html, s. 9; die KPMG Aktiengesellschaft gehört zu den führenden Wirtschaftsprüfungs- und Beratungsunternehmen und ist mit rund 11.700 Mitarbeitern an 25 Standorten präsent.
13. Bericht zur Lage der IT-Sicherheit in Deutschland 2018, S. 23 ff, www.bsi.bund.de/DE/Publikationen/Lageberichte/bsi-lageberichte.html.

14. beckonline.beck.de[4]/cont/HdbWirtschSteuerstrafR.glKap14.glA.gll.htm, Rn. 2.
15. www.divsi.de/prism-und-die-folgen-sicherheitsgefuehl-im-internet-verschlechtert/.
16. Ein „ungepatchtes“ System liegt vor, wenn es nicht mit den aktuellsten Updates versehen ist.
17. Cloud Computing beschreibt die Bereitstellung von IT-Infrastruktur und IT-Leistungen wie beispielsweise Speicherplatz, Rechenleistung oder Anwendungssoftware als Service über das Internet. Einfach ausgedrückt handelt es sich also um das Outsourcen von Soft- oder Hardware ins Internet zu einem externen Cloud Computing Anbieter.
18. BSI IT-Grundschutz Kompendium, www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/vorkapitel/Glossar_.html
19. Exploits sind eine bestimmte Art Schadprogramm. Sie enthalten Daten oder ausführbaren Code, die eine oder mehrere Sicherheitslücken in den Programmen, die auf einem Computer laufen, ausnutzen können. Drive-by-Exploits oder Drive-by-Downloads bezeichnen die automatisierte Ausnutzung von Sicherheitslücken auf einem PC. Dabei werden beim Betrachten einer Webseite ohne weitere Nutzerinteraktion Schwachstellen im Webbrowser, in Zusatzprogrammen des Browsers (Plugins) oder im Betriebssystem ausgenutzt, um Schadsoftware unbemerkt auf dem PC zu installieren.
20. Bericht zur Lage der IT-Sicherheit in Deutschland 2018, S. 23 ff, www.bsi.bund.de/DE/Publikationen/Lageberichte/bsi-lageberichte.html.
21. Eine weitere Variante sind sog. Reflection-Angriffe, wo im Internet offen vorhandene Dienste für diese Handlungen gezielt missbraucht werden.