ERLEBEN, WAS VERBINDET.

Ausführungen Dr. Kremer BKA Herbsttagung, Wiesbaden 13.11.2013

„Digitale Bedrohungen und die Maßnahmen aus Sicht der Wirtschaft“

Meine Damen und Herren,

Internetsicherheit oder in neudeutsch „Cyber Security“ ist heute ein Thema, das für die Wirtschaft von hohem Interesse ist. Das hat nicht zuletzt die Resonanz vom Cyber Security Summit am 11. November 2013 in Bonn gezeigt.

Zunächst möchte ich Ihnen einen kurzen Überblick über die Cyber Sicherheitslage, insbesondere die laufenden Angriffe auch auf das Netz der Deutschen Telekom aufzeigen, Schwachstellen und Gegenmaßnahmen benennen sowie einen Ausblick auf das weitere Vorgehen geben.

Zur Bedrohungslage in der Wirtschaft

Cyber Security ist kein Medienhype. Fast jeden Tag können wir in der Presse über neue Cyber Attacken lesen. Allein im Oktober standen mehrere Vorfälle im Fokus des öffentlichen Interesses.

Schon am 4. Oktober wurde über einen massiven Cyber Angriff auf Belgacom mit hochentwickelter Malware auf Heise.de berichtet. Es entstand der Verdacht eines neuen GCHQ Skandals. Am 07. Oktober 2013 berichtete CIO.de davon, dass gerade deutsche Webserver häufig Schadsoftware verbreiten. Diese Meldung beruhte auf Angaben des russischen Cyber Security Spezialisten Kaspersky-Lab. Der TecChannel berichtete am 15.

Oktober 2013 darüber, dass IT-Angriffe immer raffinierter werden und die Zugriffsmethoden von IT-Kriminellen auf Business Applications zur Datenbeschaffung immer ausgefeilter werden. Auch eine Häufung von Betrugsfällen beim mTAN-Verfahren durch Bankbetrüger wurde am 24. Oktober 2013 u. a. auf Zeit Online öffentlich. Dies nur als ein kurzer Überblick.

Die Angriffsziele

Die Veröffentlichungen zeigen auch, dass alle Branchen von Cyber Attacken betroffen sind. Betroffen waren Rüstungskonzerne wie Lockeed Martin oder EADS, aber auch Industriegüter Hersteller wie ThyssenKrupp oder Medienunternehmen wie für Washington Post oder die New York Times. Auch soziale Medien wie LinkedIn oder Facebook und Twitter waren von Cyber Attacken betroffen. Gleiches gilt für Internetunternehmen wie Apple und Microsoft, die Opfer erfolgreicher Angriffe waren. Die Liste ließe sich unschwer weiter fortsetzen. Der jüngste in der Presse berichtete Fall betrifft ein Datenleck bei Sky Deutschland. Hier berichtete der Spiegel noch Ende letzter Woche von einem mutmaßlichen Datendiebstahl.

Zur Identität der Angreifer

Bei dieser Vielzahl von Fällen stellt sich sofort die Frage: Wer sind eigentlich die Angreifer? Hier zeigt uns die Analyse, dass sich mehrere Typen von Angreifern identifizieren lassen. Wir unterscheiden insoweit vier Kategorien, die klassischen „Hacker“, organisierte Kriminalität, Hacktivisten und selbstverständlich auch Nachrichtendienste. Was sie alle gemeinsam haben, sind ähnliche Methoden des Vorgehens aber natürlich ganz andere Ziele.

Bei den klassischen Hackern geht es in erster Linie um das Thema Ruhm und Ehre. Sie wollen zeigen was technisch machbar ist. Es handelt sich zumeist um Einzelpersonen, die

z. B. Internetseiten verunstalten oder von ihnen entdeckte Schwachstellen in Webseiten an die Presse weitergeben oder im Rahmen von sogenannten BugBounty-Programmen den Unternehmen offen legen.

Die organisierte Kriminalität im Internet fokussiert sich auf Betrug, Erpressung und Geldwäsche. Es handelt sich um in der Regel Gruppen, die hocharbeitsteilig vorgehen. Sie sind über die ganze Welt verteilt und verfügen über hohe Finanzmittel. Ihre Tools sind z. B. Phishing Emails, die DDoS auf Onlineshops bzw. Onlinewetten, die Spam-Versendung oder ähnliches.

Ziel und Motivation von Hacktivisten ist die politische Meinungsäußerung und deren Verbreitung. Es sind in der Regel gut organisierte Gruppen, die hocharbeitsteilig vorgehen und zum Teil weltweit organisiert sind. Als Beispiele für die Aktivitäten von Hacktivisten lassen sich nennen: Anonyme Angriffe auf Unternehmen sowie die DDoS Angriffe gegen Banken, die Wikileaks Konten gesperrt hatten.

Gerade in der jüngsten Zeit sind Aktivitäten von Nachrichtendiensten besonders bekannt geworden. Ihr Ziel sind Spionage und Sabotage, sie sind staatlich gelenkt und haben sehr hohe Finanzmittel zur Verfügung. In der Presse werden als Aktivitäten von Nachrichtendiensten die Programme „Stuxnet“ und „Red October“ genannt.

Professionelles Vorgehen

Bei einer Gesamtbetrachtung der Angriffe lässt sich inzwischen feststellen, dass die Angreifer immer professioneller vorgehen. Das lässt sich anhand der organisierten Kriminalität im Internet beispielhaft erläutern. Die kriminellen Gruppen gehen oft nach demselben Muster vor: zunächst werden sogenannte Bots[1] eingeschleust, um den PC

[1] Ableitung von Roboter

eines Opfers fernsteuern zu können. Die Verteilung dieser Bots erfolgt zumeist per Spam Mail oder durch „DriveBy“ Attacken. Der mit Bots infizierte Rechner wird dann für DDoS Angriffe, Phishing von Zugangsdaten z. B. für Online-Banking oder für die Spam Versendung missbraucht. Auf diese Weise können kriminelle Gruppen es 10.000-fach ein und dieselbe Schadsoftware nutzen.

Insbesondere „PRISM“ und „Tempora“ und die Folgen

Wie unsicher und angreifbar das Internet heutzutage ist, haben auch die Vorgänge um „PRISM“ und „Tempora“ deutlich gemacht. In diesem Zusammenhang ist immer wieder die Frage gestellt worden, wie ein solches Abhören machbar ist. Wie sich Abhören technisch realisieren ließe, lässt sich klar beantworten: Bei der strategischen Fernmeldeaufklärung werden nach den Ausführungen von Edward Snowden heutzutage überwiegend Glasfaserleitungen überwacht, da die Satellitenkommunikation nur eine untergeordnete Rolle spielt. Aufgrund geologischer Gegebenheiten wie z. B. unterseeische Gebirgszüge, laufen interkontinentale Glasfaserleitungen an wenigen Knotenpunkten weltweit zusammen. Eine zentrale Überwachung ist damit technisch leicht realisierbar. Die Überwachung von Glasfaser erfolgt nach Angaben von Edward Snowden überwiegend mit optischen Splittern, die eine 1:1 Kopie der gesamten übertragenen Inhalte einer Glasfaserleitung passiv ausleiten. All das ist technisch aufwendig und erfordert ein hohes Maß an Professionalität.

Meine Damen und Herren,

Dies alles sind technische Details. Erforderlich ist aber auch eine Bewertung der Vorgänge unter dem Gesichtspunkten Datensicherheit und Datenschutz. Hierzu lässt sich fraglos feststellen, dass die vielfach geforderte Aufklärung der Sachverhalte bis heute noch aussteht. Insbesondere die Bundesregierung darf bei diesem Thema nicht locker lassen

und muss von den amerikanischen und britischen Partnern Aufklärung verlangen. Transparenz ist die wichtigste Maßnahme um verlorengegangenes Vertrauen zurück zu gewinnen, auch der Schutz der deutschen Wirtschaft für Industriespionage gehört in diesem Zusammenhang. Sogenannte No-Spy-Abkommen können diesen Schutz verstärken und sind deshalb zu begrüßen. Aber nicht nur die Unternehmen auch jeder einzelne Internetnutzer muss vor unangemessenen Abhörmaßnahmen geschützt werden. So lange die Spielregeln nicht klar sind und die Internetsicherheit nicht gewährleistet werden kann, besteht aller Anlass, über andere Schutzmaßnahmen für die Bürger in Deutschland und Europa nachzudenken. Ganz eng damit verbunden, sind Themen wie nationales Routing oder europäisches Schengen-Routing. Darüber hinaus sind einheitliche und strenge Regeln für den Datenschutz erforderlich, an die Unternehmen aus Europa und aus Übersee in gleicher Weise gebunden sind. Die seit Jahren diskutierte europäische Datenschutzgrundverordnung sollte so schnell wie möglich finalisiert und verabschiedet werden. Auch bei dem Safe-Harbour besteht deutlicher Nachholbedarf.

Werfen wir nun einen Blick auf einen weiteren sehr relevanten Aspekt zum Thema Cyber Sicherheit und das ist das immer wieder anzutreffende Problem veralteter Software.

Schwachstelle: veraltete Software

Es gibt relativ einfache Möglichkeiten, Internetangriffe zu gestalten. Angriffspunkte sind z. B. bekannt gewordene Sicherheits-Schwachstellen. Es besteht generell ein hohes Risiko, dass Software Fehler enthält. Einige Softwarefehler haben Auswirkungen auf die Sicherheit und können durch Angreifer ausgenutzt werden. Pro Monat werden durchschnittlich 400 solcher Schwachstellen bekannt. Ca. 10% der Schwachstellen sind kritisch. Natürlich gibt es neben den bekannten Schwachstellen auch andere, die unbekannt sind, da der Hersteller noch kein Software Update - also einen Sicherheitspatch - zur Verfügung gestellt hat. Und es gibt natürlich die sogenannten „Zero-

Day-Exploits“, die erst durch einen gelungenen Angriff bekannt werden. Als Beispiele für Angriffe auf Basis von bekannten Sicherheitsschwachstellen lassen sich die Fälle New York Times, Washington Post, Microsoft und Apple nennen.

Vorbeugende Sicherheitsmaßnahmen

Aber was kann man tun? Was können gerade Unternehmen tun, um aus den erfolgten Angriffen zu lernen und eigenen Systeme zu härten?

Honeypots

Bei der Telekom setzen wir dazu sogenannte Honeypots ein. Das sind Systeme, die im Internet Schwachstellen simulieren und auf diese Weise Angriffe auf sich ziehen. Die Angriffe werden dann analysiert und die gewonnenen Erkenntnisse werden zur Härtung der eigenen Systeme eingesetzt. Die Deutsche Telekom verfügt weltweit über 180 Honeypot Sensoren. Diese haben innerhalb der letzten drei Jahre rund 8,7 Millionen neue Angriffsmuster identifiziert. Pro Tag erkennen wir bis zu 800.000 Angriffe auf die Honeypots. Eine weitere Zahl ist aus meiner Sicht sehr bemerkenswert. Ein simuliertes Smartphone wurde innerhalb eines Jahres mehr als 300.000 Mal attackiert. Durchschnittlich ein Angriff pro Tag war erfolgreich. Weltweit werden derzeit fast eine Milliarde Smartphones genutzt. Das ist eine große Zahl und das damit verbundene Risiko ist nicht unerheblich. Viele Smartphone Nutzer haben sich angewöhnt, Software Updates nicht wie bei ihren PC´s zu Hause oder im Unternehmen regelmäßig aufzuspielen sondern die Smartphones eher wie Telefone zu behandeln und keine Updates vorzunehmen. Von dieser Vorgehensweise müssen wir dringend abraten, denn Smartphones sind Hochleistungsrechner, die genauso geschützt werden müssten wie unsere PC´s. Andernfalls sind sie leichte Angriffsziele.

Der Sicherheitstacho

Mit den Honeypots hat die Deutsche Telekom die Möglichkeit, ein Gesamtbild der Angriffe auf ihre Systeme in Echtzeit transparent zu machen. Das Lagebild ist für jedermann frei zugänglich über das Internet. Unter www.sicherheitstacho.eu können Sie die aktuellen Cyberangriffe verfolgen. Im Monat Oktober kamen die meisten Angriffe aus den USA, aus Großbritannien und aus Deutschland. In diesen Ländern standen die Server von denen die Angriffe ausgehen. Das Echtzeit Lagebild gibt aber keine Auskunft darüber, ob die Server Teil von Botnetzen sind und von wo aus das Botnetz gesteuert wird. Um dies heraus zu bekommen sind weitere Ermittlungen notwendig.

Trendbeobachtung und strategisches Bedrohungsradar

Die Erkenntnisse der Honeypots lassen sich zu einem strategischen Bedrohungsradar weiterentwickeln, das aktuelle Trends bei den Cyber Angriffen aufzeigt. Das strategische Bedrohungsradar der Deutschen Telekom weist drei Risikofelder auf. Die Risikofelder sind

(1) bekannte Schwachstellen, die aktiv ausgenutzt werden,
(2) vorhandene Schwachstellen deren Ausnutzung nachgewiesen ist sowie als schwächste Gruppe
(3) Bereiche, wo Schwachstellen vorhanden und jedenfalls theoretisch ausnutzbar sind.

Die Analyse der Schwachstellen wird dann kombiniert mit einer Betrachtung aus Eintrittswahrscheinlichkeit und möglicher Schaden. Daraus ergibt sich z. B., dass bei der Deutschen Telekom größtes Risiko bei Advanced persistent threats besteht.

CERT-Teams

Um mit den Cyber Risiken umzugehen, hat die Telekom ein sogenanntes Cyber Emergency Response Team oder kurz „CERT“ gebildet. Das CERT ist für die Bearbeitung

von Cyber Security Incidents wie z. B. Hackerangriffe oder kritische Schwachstellen sowie deren Prävention zuständig. Das CERT pflegt das strategische Bedrohungsradar und bildet die Schnittstelle zu Behörden, politischen Institutionen und zu internationalen Security Community.

Abuse-Management

Um die Sicherheit im Internet zu erhöhen ist auch das Verhalten der Internetnutzer, aus Sicht der Telekom der Kunden besonders wichtig.

Deshalb hat die Telekom ein sogenanntes Abuse-Management eingerichtet. Aufgabe des Abuse-Managements ist es eingegangene Hinweise auf Schwachstellen zu überprüfen und gegebenenfalls die Kunden darüber zu unterrichten. Die Telekom schickt monatlich bis 40.000 Warnschreiben an die Kunden und bittet sie, Passwörter zu ändern, Softwareupdates einzustielen oder ähnliches.

Verbesserte Sicherheit durch verstärkte Zusammenarbeit

Die genannten Beispiele stammen aus dem Bereich der Deutschen Telekom, die beim Thema Cyberangriffe sehr transparent ist. Viele andere Unternehmen sind deutlich zurückhaltender, weil sie z. B. Reputationsverluste beim Bekanntwerden von erfolgreichen Angriffen fürchten. Daher fehlt uns heute ein Gesamtbild der Sicherheitslage für Deutschland aber auch für ganz Europa. Hinzu kommt, dass das Know-how für die Abwehr von Cyber Angriffen ebenfalls ungleich verteilt ist. Unternehmen wie die Deutsche Telekom haben das Know-how, aber gerade im mittelständischen Bereich fehlt es vielfach. Daher brauchen wir insgesamt mehr Transparenz und die „Mauer des Schweigens“, die viele Unternehmen um sich errichtet haben, muss in Sachen Cyber Sicherheit eingerissen werden. Unternehmensübergreifende Kooperationen auch unter Einbeziehung der öffentlichen Hand insbesondere des Bundesamtes für Sicherheit und der

Informationstechnik sind dringend erforderlich. Die effiziente Zusammenarbeit ist ein Schlüsselfaktor für einen sicheren Cyber Standort Deutschland. Daher ist es z. B. die vom BSI und Bitkom gegründete „Allianz für Cyber Sicherheit“ sehr zu begrüßen. Diese Allianz umfasst heute schon mehr als 340 teilnehmende Institutionen und bietet eine Plattform zu Pooling von Informationen, zum Erfahrungsaustausch und zur Fort- und Weiterbildung. All das ist sehr hilfreich. Darüber hinaus ist wichtig, dass in den Unternehmen das Thema Cyber Sicherheit nicht mehr nur IT-Spezialisten überlassen wird. Angesichts der erläuterten Risiken muss klar sein, dass Cyber Security heute ein Thema für Geschäftsführungen und Vorständen der Unternehmen aus allen Branchen ist. Erforderlich ist für jedes Unternehmen eine Einschätzung der eigenen Risikolage, der Definition von daraus geleiteten Maßnahmen und selbstverständlich die zu Verfügung Stellung von sachlichen und personellen Ressourcen. In diesem Zusammenhang muss auch betont werden, dass die IT-Sicherheit auch ein Kriterium bei der Auswahl von Lieferanten sein muss.

Zusammenfassung

Cyberangriffe sind eine reale Bedrohung nicht nur für Netzwerkbetreiber, sondern für alle Unternehmen in allen Branchen.

Die Angreifer werden immer professioneller. Das gilt insbesondere für den Bereich der organisierten Kriminalität. Risiken entstehen z. B. durch veraltete Software auf Smartphones.

Die Deutsche Telekom hat Instrumente zur Früherkennung von Angriffen entwickelt (Honeypots, Sicherheitstacho, strategisches Bedrohungsradar, CERT), deren Erkenntnisse zur Härtung der Systeme eingesetzt werden. Über ein ABUSE-Management

werden Kunden informiert, wenn die Telekom eine Kompromittierung von Systemen des Kunden erkennt.

Für eine effiziente Bekämpfung der Cyberangriffe sind Transparenz und eine enge Zusammenarbeit zwischen Unternehmen und Behörden entscheidend. Bestehende „Mauern des Schweigens“ müssen eingerissen werden.