Bundeskriminalamt

HERBST-TAGUNG BKA 2013 AUTUMN CONFERENCE

Cybercrime –

Bedrohung, Intervention, Abwehr

BKA-Herbsttagung vom 12. - 13. November 2013

Digitale Bedrohungen

Langfassung

Alexander Geschonneck

Partner und Leiter des Bereichs Forensic Technology der KPMG AG

Dem Begriff Digitale Bedrohungen kann eine Vielzahl an Bedrohungen zugeordnet werden. Beispiele stellen das Ausspähen von Daten (Cyberspionage), Computersabotage und die Verletzung von Urheberrechten dar. Ein IKT-System ist hier Ziel, Werkzeug oder beides; die Bedrohungen können für Unternehmen und Behörden wie auch für Privatpersonen bestehen. Die Angriffspunkte sind entsprechend vielfältig und umfassen beispielsweise Computer, Smartphones, Industrieanlagen sowie den Bereich Connected Home.

Digitale Bedrohungen sind ebenfalls im Bereich der Wirtschaftskriminalität relevant, man spricht hier von e-Crime. Wir verstehen darunter die Ausführung von wirtschaftskriminellen Handlungen unter Einsatz von Informations- und Kommunikationstechnologien (IKT) zum Schaden einer Einzelperson, eines Unternehmens oder einer Behörde. Neben einer Schädigung von Sachwerten und einer Verletzung von Verfügungsrechten an immateriellen Gütern können diese auch aus einer Beeinträchtigung von auf den Systemen basierenden Geschäftsprozessen eines Unternehmens resultieren.

Einen Blick auf e-Crime aus kaufmännischer Unternehmensperspektive gibt die aktuelle KPMG e-Crime-Studie über Schäden in der Deutschen Wirtschaft. Gemäß der Studie war ein Viertel der befragten 500 deutschen Unternehmen in den vergangenen zwei Jahren von e-Crime betroffen, wobei in der Risikowahrnehmung der befragten Unternehmen eher die anderen Unternehmen und nicht das eigene von e-Crime betroffen sind. Computerbetrug und das Ausspähen oder Abfangen von Daten werden von Betroffenen als häufigste Deliktstypen genannt.

Die Bedrohungen werden zunehmend länderspezifisch gesehen.

Prävention als umfassende Maßnahme gegen interne und externe Bedrohungen

Es darf jedoch nicht außer Acht gelassen werden, dass die überführten Täter oft im unmittelbaren Umfeld der Unternehmen zu finden sind. Im Rahmen der Prävention müssen folglich Bedrohungen von innen wie außen berücksichtigt werden.

Die Absicherung gegen Innentäter muss dabei einem zunehmend komplexen und vernetzten Umfeld der Unternehmen Rechnung tragen und auch Personen des mittelbaren Umfeldes, wie Mitarbeiter eines beauftragten Cloud Computing- oder sonstigen Outsourcing-Dienstleisters oder von

Lieferanten, berücksichtigen. Neben der Vergabe und regelmäßigen Prüfung adäquater Zugriffsberechtigungen muss hierbei auf eine sorgfältige Auswahl und Vertragsgestaltung von Dienstleistern und Mitarbeitern geachtet werden.

Unachtsamkeit als größte Schwachstelle

Es gilt zudem zu beachten, dass nicht immer eine kompliziert auszunutzende Schwachstelle als Ursache zu sehen ist. Vielmehr sehen Unternehmen nach wie vor die Unachtsamkeit von Mitarbeitern als größte Schwachstelle im Bereich e-Crime an.

Präventionsmaßnahmen sollten daher auch regelmäßige Schulungs- und Sensibilisierungsmaßnahmen umfassen, die die Wahrscheinlichkeit unabsichtlich durch Mitarbeiter hervorgerufener Schwächen im Bereich der IT-Sicherheit deutlich reduzieren können. Schulungs-Umfang und -Taktung müssen hierbei der Rolle der Person angepasst werden. Weiterhin müssen im Rahmen der Präventionsmaßnahmen neue Technologien berücksichtigt werden; so sollte geprüft werden, ob hinsichtlich der Nutzung sozialer Netzwerke in angemessenem Umfang formelle Regelungen getroffen werden sollen.

Wichtig ist auch die Verbesserung der Meldung und Eskalation von Sicherheitsvorfällen innerhalb der Unternehmen, da „Kommissar Zufall“ immer noch die häufigste Meldequelle darstellt.

Verschiedene Faktoren können (Cyber-) kriminalität begünstigen

Faktoren, die (Cyber-) kriminalität begünstigen, zeigt das sogenannte „Fraud Triangle“ des US-amerikanischen Soziologen und Kriminologen Donald R. Cressey auf. Es umfasst die Faktoren Gelegenheit, Motivation und Rechtfertigung.

Der Faktor Gelegenheit wird dabei auf der Organisationsebene verortet. Schwächen interner Kontrollsysteme führen zu fehlenden oder unzureichenden Kontrollen, die von Tätern als Gelegenheit wahr genommen werden. Motivation und Rechtfertigung hingegen ordnet Cressey der Personenebene zu. Beeinflussend wirkt hier das Wertesystem des Unternehmens und der sogenannte „Tone from the top“.

Der Faktor Motivation kann dabei durch die Persönlichkeit sowie finanzielle und tätigkeitsbezogene Gegebenheiten beeinflusst werden. So kann eine problematische finanzielle Situation eines Mitarbeiters Motivation sein, kriminelle Taten zu begehen. Der Faktor Rechtfertigung wird durch die Persönlichkeit, aber auch unternehmenskulturell beeinflusst. So kann eine als problematisch empfundene Unternehmenskultur als Rechtfertigung krimineller Taten dienen.

Beispiele aus dem Innenleben eines Unternehmens

In der forensischen Praxis trifft man auf eine Vielzahl von Beispielen im Kontext digitaler Bedrohungen.

Ein Beispiel stellt die Manipulation von Warenwirtschaftssystemen dar. Gewähren die eingerichteten Benutzerrechte in Warenwirtschaftssystemen für Nutzer zu umfangreiche Rechte, können diese beispielsweise unbemerkt Lagerbestände manipulieren oder eine Zahlung an einen fiktiven Lieferanten ohne Lieferung durchführen.

Eine Detektion kann anhand einer Überprüfung von Massendaten mittels Datenanalysen erfolgen. Ebenso können Analysen des Berechtigungssystems Schwächen aufzeigen, die beispielweise die vollumfängliche Durchführung von Transaktionen durch eine Person, aufgrund einer fehlenden Funktionstrennung, ermöglichen.

Als weiteres Beispiel können externe Callcenter oder andere externe Dienstleister genannt werden, die aufgrund der vorhandenen umfangreichen vertraulichen Daten ein potentielles Ziel von Datendieben darstellen. Neben einem Diebstahl durch externe Personen ist hier insbesondere auch an einen Diebstahl von Datensätzen durch Mitarbeiter zu denken. Die Daten werden dann zum Beispiel weiterverkauft oder vom Täter im Kontext eines Identitätsmissbrauchs selbst genutzt.

Im Rahmen der Detektion ist zu beachten, dass ein Zugriff auf die vertraulichen Daten für bestimmte Mitarbeitergruppen zur Arbeitserledigung erforderlich ist. Der Zugriff auf vertrauliche Daten muss entsprechend der gegebenen Erfordernisse definierten Personengruppen grundsätzlich erlaubt sein. Es ist jedoch zielführend, dass Systeme zum Zugriff auf diese Daten einen unbegründeten Zugriff auf eine hohe Anzahl von Datensätzen verhindern oder diesen zumindest melden.

Es gibt zahlreiche weitere Beispiele. So seien hier noch das Rogue Trading, das heißt die Manipulation von Handelsplattformen im Bereich des Investment- oder auch Commodity-Tradings sowie Angriffe auf Zahlungsverkehrssysteme genannt.

Evolution von Bedrohungen

Ist mittels geeigneter Präventionsmaßnahmen ein angestrebtes Schutzniveau erreicht, darf dieses nicht als abschließende Zielerreichung angesehen werden. Perspektivisch kann das Schutzniveau vielmehr durch die Weiterentwicklung bestehender Bedrohungen und die Entstehung neuer Bedrohungen sinken.

So ist eine Professionalisierung der Angriffe und der hierfür genutzten Werkzeuge zu beobachten. Ein Geschäftsmodell stellt es beispielsweise dar, hochentwickelte Angriffswerkzeuge zu erstellen und Dritten gegen eine Gebühr zur Verfügung zu stellen. Dies geht so weit, dass „betriebsfertige" Lösungen als Cracking-as-a-Service angeboten werden. Ein Beispiel stellt das Malware-Toolkit „Blackhole" dar.

Mittels dieser Lösung können Dritte auf gehackten oder für diesen Zweck extra erstellten Webseiten Malware einbringen und so Webseitenbesucher mit dieser Malware infizieren. Hierzu prüft „Blackhole" das System des Besuchers auf Sicherheitslücken und nutzt gefundene Lücken aus. Der Angreifer kann bei Erfolg beispielsweise Daten auf dem Rechner des Opfers ausspähen oder die Rechner in Form eines Botnetzes zusammenfassen. „Blackhole" verfügt über eine grafische Bedienoberfläche, die Nutzern unter anderem diverse Konfigurationsmöglichkeiten sowie eine Auswertung hinsichtlich erfolgreicher Angriffe zur Verfügung stellt.

Die Detektion eines solchen Angriffs kann (etwas) verbessert werden, wenn Unternehmen mehrere Malware-Scanner kombinieren, um die Erkennungsrate zu steigern.

Botnetze

Beispielsweise als Resultat eines gezielten Angriffs mittels des vorgenannten „Blackhole"-Toolkits kann ein Angreifer Zugriff auf eine Vielzahl infizierter Rechner erhalten und diese zu

einem sogenannten Botnet zusammengeführen. Bei Botnetzen handelt es sich um zentral gesteuerte mit Malware infizierte Rechner.

Botnetzbetreiber vermieten Ihre Botnetze oftmals an Dritte, die damit bspw. andere Rechner oder Rechnernetze überlasten können (DDoS) oder SPAM versenden. Mittels der Drohung mit einem DDoS-Angriff kann digitale Erpressung ein Geschäftsmodell darstellen. Eine Detektion ist erst zum Zeitpunkt eines Angriffs möglich, sollte es nicht zur Androhung eines Angriffs im Rahmen einer Erpressung kommen. Gegenmaßnahmen sind aufgrund der hohen Zahl angreifender Rechner aufwändig und betreffen insbesondere die Filterung unerwünschter Anfragen. Es verbleibt so primär die normale Detektion der befallenen Bot-Systeme.

Gezielte Angriffe auf Unternehmen und Datenbestände

Neben ungezielten Angriffen ist eine steigende Zahl gezielter Angriffe auf Unternehmen und Datenbestände zu beobachten. Bei diesen sogenannten „Targeted Attacks“ werden ausgesuchte Ziele angegriffen und ausgesuchte Informationen erbeutet.

Hierbei kommt es zum Teil zu sogenannten „Advanced Persistent Threats“ (APTs), das heißt zu anhaltenden Angriffen. Üblicherweise gehen APTs nicht von einzelnen Tätern, sondern von Tätergruppen aus. Es wird nicht während eines kurzen Angriffs so viel wie möglich erbeutet, sondern der Zugriff auf das Ziel möglichst lang aufrecht erhalten.

Als Beispiele für gezielte Angriffe können u. a. der Angriff auf das belgische Telekommunikationsunternehmen Belgacom ab dem Jahr 2010 sowie der Angriff auf die Sicherheitsfirma Bit9 durch die Hackgruppe „Hidden Lynx“ genannt werden. Letzterer diente als Vorbereitung für Angriffe auf Kunden von Bit9 in der Rüstungsindustrie.

Es wird jedoch nicht allein auf die Methoden des Crackings zurückgegriffen. Zusätzlich wurden bekannte Angriffsmethoden in Richtung gezielter Angriffe modifiziert.

So wird beispielsweise das bekannte Phishing als „Spear Phishing“ zu einer gezielten Angriffsmethode. Hierbei werden Methoden des Social Engineering gegen ausgesuchte Personen wie Mitarbeiter mit Administrationsrechten oder Mitglieder der Führungsebene eines Unternehmens (sog.

„Whaling“) eingesetzt. Für Angreifer verspricht dieses Vorgehen eine höhere Erfolgsquote, ein Profiling ist oft recht einfach mittels beruflicher und privater sozialer Netzwerke möglich. Angreifer können durch diese minimal invasiven Angriff länger unentdeckt bleiben, als wenn Sie mit tausenden Phishingmail an den Sicherheitssystemen abprallen. So konnten mittels Zugangsdaten, die durch Phishing erlangt wurden, Angreifer im Jahr 2011 in den Handel mit Emissionszertifikaten eingreifen.

Eine automatisierte Detektion dieser Angriffe ist aufgrund wechselnder Texte und gefälschter Absender schwierig. Es ist daher eine Sensibilisierung der Mitarbeiter hinsichtlich der Methoden des Social Engineering zu empfehlen.

Ein Angriffziel stellen zudem Industriesteuerungsanlagen dar. Diese verfügen oftmals über einen Anschluss an das Internet, bspw. zur Fernwartung. Erhält ein Angreifer Zugriff auf eine Industriesteuerungsanlage, kann dieser genutzt werden, um Informationen zu erlangen und die Anlagen zu manipulieren, zu beschädigen oder zu zerstören. Für diese Anlagen sollte daher genau geprüft werden, ob ein Anschluss an das Internet oder damit verbundene Netzwerke erforderlich ist.

Eine Sicherheitslücke kann schnell eine hohe Anzahl dieser Systeme verwundbar machen. So wies die Steuerungssoftware eines Hersteller im Jahr 2012 eine Sicherheitslücke auf, mittels derer eine Manipulation der Steuerung zugehöriger Systeme möglich war. Allein diese Steuerungssoftware wurde von über 250 Geräteherstellern genutzt, die u. a. Firmen im Energie- und Militärbereich beliefern.

Eine Suche mittels der auf Server spezialisierten Suchmaschine „Shodan“ nach Systemen, deren Statusmeldungen unter anderem den für Steuerungstechnik charakteristischen Term „SCADA“ (Supervisory Control and Data Acquisition) zurückliefern, listet eine Vielzahl von Systemen auf. Wenngleich bereits länger bekannt ist, dass eine solche Suche einfach möglich ist, finden sich unter diesen Systemen auch heute einige Systeme, die diverse Informationen ohne Anmeldung zur Verfügung stellen. Wenngleich diese Informationen keine Steuerung der Systeme ermöglichen, können beispielsweise Informationen zu vorhandenen Benutzerkonten Angriffe auf die Systeme erleichtern.

Entstehung neuer Bedrohungen durch neue Technologien

Die zunehmende Nutzung neuer Technologien hat auch zur Entstehung neuer Bedrohungen geführt.

So haben sich beispielsweise die Infektionswege von Malware im Zeitverlauf geändert. Zu Anfang stellten oftmals externe Datenträger das Transportmedium für Malware dar. Kam es zuerst zu einer Installation von Bootsektor-Viren durch infizierte Floppydisks, folgte eine hohe Zahl von Infektionen mittels des Anschlusses von externen Datenspeichern wie externen Festplatten und USB-Sticks.

Die zunehmende Verbreitung von E-Mail hatte später auch zu einem massenhaften Versand von Malware als Anhang von E-Mails zu Folge, die zu einer Infektion durch Ausführung von E-Mail-Anhängen führte.

Inzwischen stellen Drive-By-Downloads und eine Ansprache durch soziale Netzwerke ein Einfallstor für Infektionen dar. Es kommt dabei zu einer unbemerkten Installation von Malware, die lediglich den Besuch einer infizierten Webseite erfordert und Sicherheitslücken bspw. im Microsoft Internet Explorer und Adobe Flash ausnutzt. Als Verbreitungsmedium dienen gehackte Webseiten oder Accounts in Social Networks; da es sich oftmals um gehackte seriöse Accounts und Webseiten handelt, ist die Gefahr einer Infektion besonders hoch.

Sicherheitsmaßnahmen wie Malware- und Webfilter reichen bei dieser Bedrohung oftmals nicht aus, da die URLs und Signaturen der Malware sich sehr häufig ändern. Es ist daher auch hier sehr wichtig, Mitarbeiter zu sensibilisieren.

Weiterhin werden mobile Endgeräte mit steigender Leistungsfähigkeit zu interessanten Zielen. Funktionalitäten wie GPS-Ortung ermöglichen neue Angriffsszenarien wie beispielsweise eine heimliche Verfolgung der Nutzer; die Installation von Apps birgt das Potential der Installation unerwünschter Funktionalitäten. Es gibt Smartphoneplattformen, bei denen davon ausgegangen werden kann, dass die Mehrheit der auf dem Markt befindlichen Geräte erfolgreich kompromittiert wurden.

Für Unternehmen entsteht in diesem Fall insbesondere dann eine Bedrohung, wenn sie dem Trend zu „Bring-Your-Own-Device“ folgen und als Folge auch privat genutzte Endgeräte im Unternehmensnetzwerk aktiv sind und Zugriff auf sensible Daten damit erfolgen soll. Fehlt ein adäquates Sicherheitskonzept, können Schädlinge durch Bring-Your-Own-Device (BYOD) ihren Weg in das Firmennetzwerk finden.

Die mobile Telekommunikation wird als risikobehaftetste IT-Anwendung für Unternehmen angesehen. Allein für das erste Quartal 2013 meldet F-Secure 149 neue Malwares für mobile Endgeräte; 136 davon zielen auf das von Google entwickelte Betriebssystem Android ab.

Cloud Computing

Auch die zunehmende (private und geschäftliche) Nutzung von Public und Private Clouds bringt Bedrohungen mit sich.

Problematisch ist hierbei, dass das Sicherheitsniveau der Cloud-Dienste nicht immer feststellbar ist. Weiterhin wird eine Detektion von Angriffen in vielen Fällen durch den Cloud-Dienstleister erfolgen müssen. Auffälligkeiten sollten folglich dem Dienstleister gemeldet werden, um die Detektion eines Angriffs zu unterstützen.

Beispiele für erfolgreiche Angriffe stellen der Zugriff auf Dropbox-Konten durch Dritte nach der Kompromittierung eines Mitarbeiter-Accounts im Jahr 2012 sowie der Zugriff auf Evernote-Passwort-Hashes von 50 Millionen Nutzern durch Dritte im Jahr 2013 dar.
Das Cloud Computing kann neben einem Ziel auch ein Werkzeug für Cyberkriminelle darstellen. Sie können die schnell verfügbare hohe Rechenleistung von Cloud-Diensten beispielsweise nutzen, um Passwörter zu „knacken“.

Adäquate Prävention als Wettbewerbsvorteil

Es kann festgehalten werden, dass die Zahl und Intensität Digitaler Bedrohungen weiter zunimmt. Neben der Evolution bestehender Bedrohungen entstehen neue Bedrohungen, deren Wirkung aufgrund der Neuheit der damit verbundenen Technologien noch nicht ausreichend abgeschätzt werden kann. Die Täter, deren kommerzielles Interesse sehr groß ist, werden immer weiter versuchen,

lange unerkannt zu bleiben. Die zunehmende Professionalisierung Digitaler Bedrohungen führt zu einer Ausweitung der Gruppe potentieller Täter sowie einer zunehmend schwierigen Erkennung von Angriffen.

Die zunehmende Nutzung Sozialer Netzwerke, die Internetnutzung mit mobilen Endgeräten sowie das Cloud Computing eröffnen neue Möglichkeiten für Angreifer; neue Technologien sollten daher nicht unvoreingenommen genutzt und ggf. reguliert werden. Zunehmend gezielte Angriffe führen zu höheren Erfolgsquoten für Angreifer und erfordern eine stärkere Sensibilisierung von Mitarbeitern.

Für Unternehmen wird eine umfangreiche Prävention daher zunehmend einen Wettbewerbsvorteil darstellen. Unverzichtbar ist jedoch auch eine Zusammenarbeit von Unternehmen, beispielsweise bei der Erkennung branchenspezifischer Angriffe. Erfolgreiche Angriffe können zu erheblichen Kosten führen, bei denen auch Reputationsschäden nicht außer Acht gelassen werden dürfen.

Die Prävention darf dabei nicht auf die Umsetzung von Maßnahmen zur Erkennung von Angriffen beschränkt werden. Zusätzlich muss bereits vor einem Schadensfall geklärt werden, ob ein Unternehmen gewappnet ist, im Fall der Erkennung eines aktiven Angriffs diesen einzudämmen und aufzuklären. Da Angriff (auch erfolgreiche) nicht unvermeidlich sein werden, werden die Unternehmen auf Dauer erfolgreich sein, die angemessen reagieren können.