Bundeskriminalamt

HERBST-TAGUNG BKA AUTUMN CONFERENCE 2013

# Cybercrime –

# Bedrohung, Intervention, Abwehr

BKA-Herbsttagung vom 12. - 13. November 2013

## Digitale Bedrohungen

Kurzfassung


**Alexander Geschonneck**

Partner und Leiter des Bereichs Forensic Technology der KPMG AG Wirtschafts-prüfungsgesellschaft in Berlin

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.

Digitale Bedrohungen sind ebenfalls im Bereich der Wirtschaftskriminalität relevant, man spricht hier von e-Crime. 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 die Bedrohungen zunehmend länderspezifisch gesehen werden.

## 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.

## 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. Hierzu gehört auch die Ver-

besserung der Meldung von Sicherheitsvorfällen innerhalb der Unternehmen, da „Kommissar Zufall“ immer noch die häufigste Meldequelle darstellt.

## Evolution von Bedrohungen

Ist mittels geeigneter Präventionsmaßnahmen ein angestrebtes Schutzniveau erreicht, darf dieses nicht als abschließende Zielerreichung angesehen werden. Perspektivisch kann wird 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.

## Gezielte Angriffe auf Unternehmen und Datenbestände

Weiterhin steigt die Zahl gezielter Angriffe auf Unternehmen und Datenbestände. Dabei wird 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.

## Entstehung neuer Bedrohungen durch neue Technologien

Neue Bedrohungen entstehen aus der zunehmenden Nutzung neuer Technologien. So 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.

## 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.

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 Angriffe (auch erfolgreiche) nicht unvermeidlich sein werden, werden die Unternehmen auf Dauer erfolgreich sein, die angemessen reagieren können.