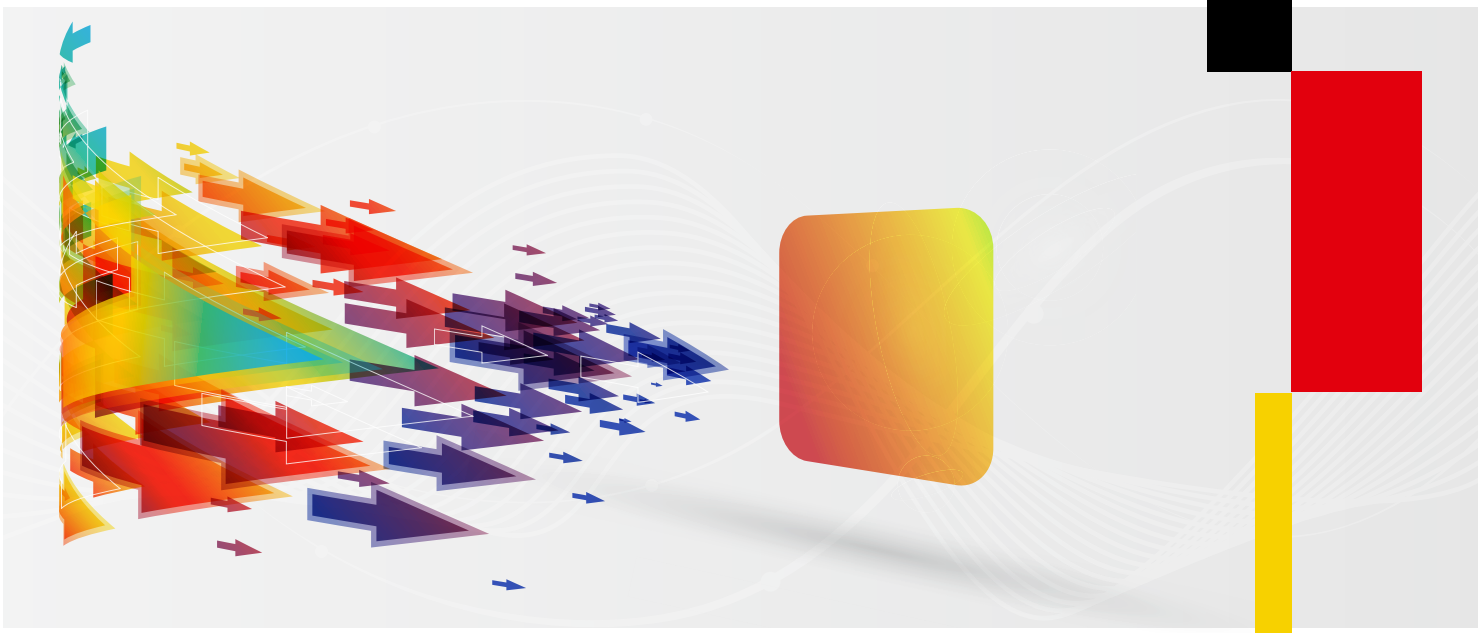
Bundesamt
für Sicherheit in der
Informationstechnik

Die Lage der IT-Sicherheit in Deutschland 2011



Bundesamt für Sicherheit in der Informationstechnik
www.bsi.bund.de

Inhalt

Vorwort

Michael Hange
Präsident des Bundesamtes für Sicherheit in der Informationstechnik

Die Chancen, die uns die heutige Informationstechnik im privaten und beruflichen Umfeld bietet, sind groß. Ebenso groß sind aber auch die Risiken, die sich mit der zunehmenden Verlagerung von Geschäftstätigkeiten und sozialer Interaktion in die virtuelle Welt ergeben.

Denn auch die Angreifer lernen dazu und entwickeln ausgefeilte Methoden, die ihnen einen Vorsprung vor den potenziellen Opfern verschaffen. Autoren von Schadsoftware setzen zunehmend verschiedene technische Maßnahmen ein, um die Erkennung oder Analyse ihrer Programme zu erschweren. So gibt es beispielsweise Schadprogramme, die das zu infizierende System auf Merkmale einer Analyse-Umgebung untersuchen. Werden solche erkannt, wird die Infektion abgebrochen. Eine Analyse des Programms durch Spezialisten ist somit erschwert. Dadurch steigen die Anforderungen an die Nutzer, und ihre aktive Mitwirkung wird noch wichtiger, als sie es ohnehin bislang war. Wachsamkeit und neugieriges Hinterfragen muss im Netzalltag so selbstverständlich werden, wie es auch in der Offline-Welt der Fall ist.

Längst haben Hacker für ihre Dienste einen Markt etabliert und die „Verdienstmöglichkeiten“ für Internetkriminelle verbessert. Ein Botnetz mit 10.000 Bot-PCs lässt sich beispielsweise für rund 200 US-Dollar pro Tag mieten. Da Botnetze auch aus mehreren Millionen PCs bestehen können, lässt sich das monetäre Potenzial hinter solchen Internetangriffen nur erahnen.

Entmutigen lassen wir uns dadurch nicht, denn erfreulicherweise sind immer wieder Erfolge zu verzeichnen. Sie resultieren etwa aus der Zerschlagung großer Botnetze. Oftmals ist dies ein gemeinsamer Erfolg vieler Unternehmen, IT-Sicherheitsinstitutionen und Ermittler rund um den Globus. Die weltweite Vernetzung wird weiter ausgebaut. Mit dem Nationalen Cyber-Abwehrzentrum, welches am 1. April unter Federführung des BSI seine Arbeit aufgenommen hat, ist eine Kooperationseinrichtung deutscher Sicherheitsstellen auf Bundesebene geschaffen worden, deren Aufgabe die Abwehr elektronischer Angriffe auf IT-Infrastrukturen des Bundes und kritische Infrastrukturen der Wirtschaft ist.

Meine Mitarbeiter und ich leisten unseren Beitrag dazu, die Online-Welt für uns alle sicherer zu machen. Daran arbeiten wir mit großem Engagement.

Bonn, im Mai 2011

Ihr Michael Hange

Überblick

Zahlreiche Prozesse und Aufgaben in Verwaltung und Unternehmen sind heute IT-gestützt. Auch im privaten Umfeld sind für die meisten Deutschen der PC und das Mobiltelefon nicht mehr wegzudenken. Wirtschaft, öffentlicher Sektor sowie Bürgerinnen und Bürger sind damit in hohem Maße von einer funktionierenden Informationstechnik und sicheren Informationsinfrastrukturen abhängig.

Organisierte Kriminalität aber auch Nachrichtendienste führen heute hoch professionelle IT-Angriffe auf Firmen, Behörden und auch auf Privatpersonen durch. Die Methoden werden immer raffinierter, und die Abwehr von Angriffen erfordert einen immer höheren Aufwand. So griff etwa das Trojanische Pferd „Stuxnet“ gezielt Prozesssteuerungssysteme an. Die Art und Weise, mit der seine Programmierung erfolgte, erfordert einen sehr hohen Aufwand und hochspezialisiertes Wissen auf Seiten der Angreifer. Angriffe auf IT-Systeme gab es schon immer, jedoch hat sich deren Intensität und Charakter verändert. Zu der quantitativ hohen Zahl der Angriffe kommt eine neue Qualität zielgerichteter Attacken hinzu. Dabei lässt sich feststellen, dass für Angriffe auf die breite Masse vor allem Standardschwachstellen – wie etwa bei Werbebannern – genutzt werden. Geheime, beziehungsweise bislang unentdeckte Schwachstellen, werden für gezielte Cyber-Attacken eingesetzt. Die Angreifer „verschwenden“ ihr Wissen nicht. Entsprechend sind seit Erscheinen des letzten Berichts aus dem Jahr 2009 die Methoden der Angreifer noch arglistiger geworden. Neben den Schwachstellen in Betriebssystemen sind es Sicherheitslücken in Anwendungsprogrammen und Softwarekomponenten von Drittanbietern, die von Angreifern ausgenutzt werden. Auch gezielte Angriffe, die individuell auf bestimmte Personen zugeschnitten sind und zur Tarnung einen hohen Aufwand an Social Engineering einsetzen, haben zugenommen.

Die Anzahl neuer Schadprogramme nimmt ebenfalls weiterhin sehr stark zu. Allerdings werden sie nicht mehr wahllos in großen Wellen im Internet gestreut. Oft sind weltweit nur wenige Rechner von demselben Schadprogramm betroffen, was die Erkennung extrem erschwert.

Klassisches Phishing ist praktisch nicht mehr fest zu stellen. Das bedeutet jedoch nicht, dass Identitätsdiebstahl keine Bedrohung mehr darstellt – im Gegenteil. Hier hat sich ein kriminelles Betätigungsfeld entwickelt, welches professionalisierte Strukturen aufweist.

Beim Thema Spam lässt sich beispielhaft die Zielorientierung der Angreifer erkennen. Die Menge hat sich zwar verringert, dafür werden Spams zielgerichteter eingesetzt, wodurch das Gefährdungspotenzial unvermindert hoch bleibt.

Für die mit der Schadcode-Analyse betrauten Sicherheitsexperten wird die Arbeit zunehmend zu einem Wettlauf, den sie sich mit den Angreifern liefern. Positiv ist die sich stetig verbessernde Kooperation zwischen Herstellern, Providern und Sicherheitsexperten. Durch

gemeinsame Initiative konnte zum Beispiel die Abschaltung gefährlicher Botnetze erreicht werden. Auch im Bereich der CERTs existiert mit dem Forum of Incident Response and Security Teams (FIRST) ein internationales Netzwerk. Insgesamt wurde erkannt, dass gemeinschaftliches Handeln einen Gewinn für alle Beteiligten bedeutet – jedoch wird weiterhin eine Steigerung der Bemühungen aller erforderlich sein, um die Gesamtlage unter Kontrolle zu haben.

Eine zunehmende Herausforderung liegt in der raschen Verbreitung von Smartphones, Netbooks und Tablet-PCs, durch die die Angriffsfläche für Cyber-Kriminelle erheblich vergrößert wurde. Unterstellt man Internetangriffen ein finanziell lohnendes Geschäftspotenzial bei vergleichsweise geringem Risiko einer Bestrafung, ist es wahrscheinlich, dass Angriffe künftig noch zunehmen.

Es ist anzunehmen, dass das Trendthema Cloud Computing aufgrund seines Potenzials zur Kostenreduktion und zur Steigerung der Verfügbarkeit eine zunehmende Verbreitung erfährt. Dabei wird die Gewährleistung der Informationssicherheit eine neue internationale Dimension erreichen, denn die Daten verlassen den Rechtsraum der Bundesrepublik. Eine stärkere internationale Zusammenarbeit wird immer notwendiger. Genau wie durch die Omnipräsenz von IT-Systemen im Alltag – künftig beim Thema Smart Grid/Smart Meter zu erwarten – werden Verantwortliche verstärkt vor organisatorische Herausforderungen, zum Beispiel im Bereich des Risikomanagements, gestellt.

Gefährdungstrends

Bedrohung	2009	2011	Prognose
DDoS-Angriffe	↑	→	→
Unerwünschte E-Mails (Spam)	↑	→	→
Botnetze	↑	↑	↑
Identitätsdiebstahl	↑	↑	↑
Sicherheitslücken	–	↑	↑
Drive-By-Exploits	–	↑	→
Schadprogramme	–	↑	↑

Quelle: BSI

Abb. 1: Entwicklung von IT-Bedrohungen nach Einschätzung des BSI [7]

Risikopotenzial für Angriffsmöglichkeiten in ausgewählten Anwendungen und Technologien

Technologie/Anwendung	2009	2011	Prognose
Mobilkommunikation	↑	↑	↑
SCADA	↑	↑	↑
DNS und BGP	↑	↑	→
Schnittstellen und Speichermedien	→	↑	↑

Quelle: BSI

Abb. 2: Risikopotenzial für Angriffsmöglichkeiten in ausgewählten Anwendungen und Technologien nach Einschätzung des BSI [7]

Risikoprofil innovativer Anwendungen und Technologien

Technologie/Anwendung	2009	2011	Prognose
Cloud Computing	–	↑	↑
Smart Grid/ Smart Meter	–	↑	↑

Quelle: BSI

Abb. 3: Risikoprofil innovativer Anwendungen und Technologien nach Einschätzung des BSI [7]

↑ steigend ↓ sinkend → gleichbleibend

1 Sicherheitslücken

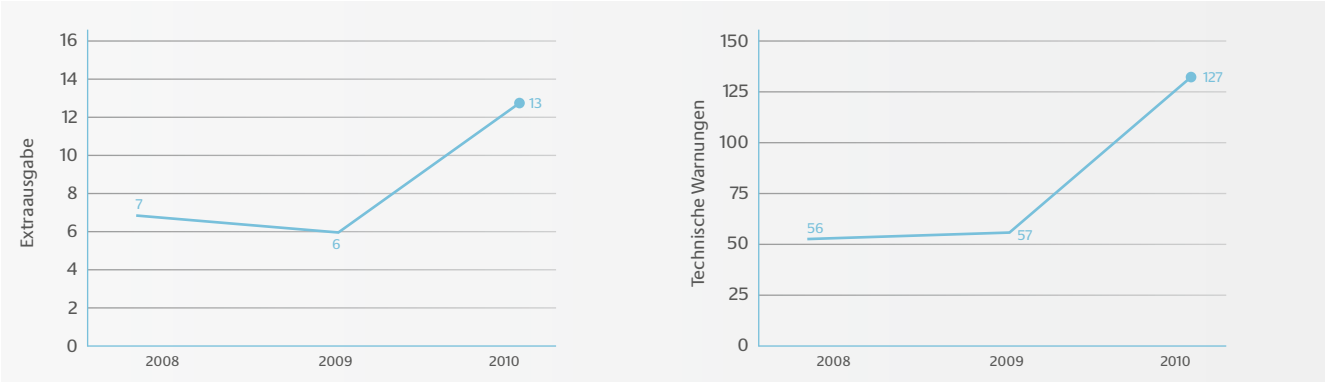
Die Zahl der veröffentlichten Sicherheitslücken war im Jahr 2010 weiterhin hoch. Ob dieser Trend auch für 2011 zu erwarten ist, bleibt offen. Genaue Zahlen lassen sich kaum erheben, denn die Dunkelziffer nicht öffentlich gemachter Schwachstellen ist unbekannt. Hierbei spielt auch eine Rolle, dass Sicherheitslücken von einigen Herstellern zum Teil heimlich über so genannte „Silent Fixes" behoben werden können und somit nicht in die Statistik einfließen.

Software-Schwachstellen nehmen zu

Für den typischen Endnutzer-PC sind Veränderungen im Verhältnis zwischen der Anzahl der Schwachstellen im Betriebssystem und der in Drittanbieter-Software auffällig. Während Sicherheitslücken in Betriebssystemen (wie Microsoft Windows) für Angreifer zunehmend an Bedeutung verlieren, ist die Anzahl der Schwachstellen in Drittanbieter-Software 2010 stark gewachsen. [1] Dies ist insbesondere kritisch, wenn man den hohen Verbreitungsgrad vieler Anwendungen berücksichtigt. Der Adobe Flash Player beispielsweise befindet sich nach Herstellerangaben auf über 99 Prozent aller PCs in Europa und war im Jahr 2010 laut CVE[1] von 60 Schwachstellen betroffen, von denen 53 zur Ausführung von Schadcode ausgenutzt werden konnten. Der Webbrowser Mozilla Firefox liegt in Europa bezüglich des Marktanteils mittlerweile an der Spitze. [2] Er wies 2010 laut CVE 107 Schwachstellen auf, davon ermöglichten 60 Schadcodeausführung. Die potenzielle Angriffsfläche steigt folglich mit jeder genutzten Anwendung weiter an.

Der Warn- und Informationsdienst „Bürger-CERT" des BSI verzeichnet einen stetigen Anstieg an Meldungen, die vor zeitkritischen Sicherheitslücken warnen. So wurden in der „Extraausgabe" des Newsletters im Jahr 2010

Gemeldete Sicherheitslücken



Quelle: BSI

Abb. 4: Anzahl der vom Bürger-CERT gemeldeten zeitkritischen Sicherheitslücken und der vom CERT-Bund versendeten „Technischen Warnungen" [7]

[1] Die „Common Vulnerabilities and Exposures" (CVE) sind ein industrieweit anerkannter Standard zur einheitlichen Katalogisierung von Schwachstellen in IT-Systemen

insgesamt 13 Warnungen veröffentlicht, mehr als in den Jahren zuvor. Seit 2008 lässt sich auch ein kontinuierlicher Anstieg der „Technischen Warnungen“ durch das „Bürger-CERT“ beobachten.

Die Software-Hersteller haben ihre Mitverantwortung für die IT-Sicherheit erkannt und arbeiten aktiv daran, ihre Produkte zu verbessern. Sicherheitslücken werden deshalb nicht mehr nur ausschließlich von Dritten „entdeckt“, sondern auch von den Herstellern selbst gemeldet. Zeit bleibt aber nach wie vor ein kritischer Faktor. Zero-Day-Angriffe, bei denen Schwachstellen bereits am Tag ihres Bekanntwerdens ausgenutzt werden, sind mittlerweile die Regel. Gleichzeitig birgt die große Anzahl fortlaufend neu entdeckter Schwachstellen die Gefahr, dass die Hersteller dieser Entwicklung nicht mehr folgen können und Sicherheitslücken über lange Zeiträume bestehen bleiben. So waren mit Stand vom 15. Februar 2011 laut CVE beispielsweise in verschiedenen Microsoft-Produkten (Windows, Office, Internet Explorer) über 20 Lücken öffentlich bekannt, 16 davon ermöglichten die Ausführung von Schadcode. Ein Großteil wurde dabei bereits seit mehreren Wochen beschrieben.

Zentrale Patches helfen

Vor diesem Hintergrund müssen auch effektive Aktualisierungs-Mechanismen gefordert werden, um Sicherheitslücken wirksam und schnell zu beheben. Automatische Update-Funktionen haben sich hierbei als sehr hilfreich erwiesen. Dabei wird Software nach Möglichkeit ohne Zutun des Anwenders auf dem aktuellen Stand gehalten, indem sicherheitsrelevante Aktualisierungen eingespielt werden, sobald sie verfügbar sind. Derartige Funktionen befinden sich mittlerweile in den meisten verbreiteten Anwendungen. Doch auch hier existieren Probleme: Da es an zentralen Update-Funktionalitäten mangelt, verwenden die Anwendungen typischerweise einen eigenen spezifischen Aktualisierungsmechanismus und -rhythmus. Teilweise existieren hier sogar große Unterschiede zwischen Produkten eines einzigen Herstellers. Außerdem bieten einige Hersteller die Aktualisierungen nicht zeitnah an, sondern setzen auf so genannte „Patch Days“, bei denen es sich um feste Termine für die Veröffentlichung von Patches handelt. Schlimmstenfalls bestehen Sicherheitslücken dann zwischen einem (derzeitiger Patchzyklus bei Microsoft) und drei Monaten (derzeitiger Patchzyklus bei Adobe). Hersteller sind daher immer häufiger gezwungen, bei kritischen Lücken mit vorläufigen Maßnahmen („Workarounds“) zu reagieren, die zusätzlichen Aufwand auf Seiten der Anwender und Administratoren erfordern. Oftmals werden aber auch Patches für besonders kritische Lücken außerplanmäßig vorgezogen.

Das BSI steht daher mit den großen Software-Herstellern in ständigem Kontakt, um die Entwicklung zentraler Aktualisierungsmechanismen weiter voranzutreiben sowie sicherzustellen, dass Updates zeitnah verfügbar sind. Aktualisierungen sollten zukünftig unmittelbar bei Verfügbarkeit vollautomatisch eingespielt werden können, um mit der Bedrohungslage durch immer neue Sicherheitslücken Schritt zu halten. In administrierten Umgebungen müssen solche Mechanismen durch die Administratoren sicher gestellt werden.

Fazit:

Die Bedrohung durch Schwachstellen in Software-Produkten befindet sich auf einem sehr hohen Niveau und steigt weiter. Diese Situation wird verschärft durch lange Zeiträume, in denen keine Patches für öffentlich bekannte und teilweise kritische Schwachstellen verfügbar sind. Zeitnahe Updates, die zentral und automatisch eingespielt werden können, sind daher unbedingt erforderlich.

2 Drive-By-Exploits

Drive-By-Exploits

So genannte Drive-By-Exploits bezeichnen die automatisierte Ausnutzung von Sicherheitslücken auf einem PC. Dabei werden beim Betrachten einer Webseite ohne weitere Nutzerinteraktion Schwachstellen im Browser, in Browser-Plugins oder im Betriebssystem ausgenutzt, um Schadsoftware wie Trojanische Pferde unbemerkt auf dem PC zu installieren.

Wie wichtig es ist, Sicherheitslücken in Software-Produkten umgehend zu schließen, zeigt sich exemplarisch in der Möglichkeit, durch so genannte Drive-By-Exploits den eigenen Rechner quasi im „Vorbeisurfen“ zu infizieren. In der Vergangenheit waren entsprechende Schadprogramme hauptsächlich auf dubiosen Webangeboten zu finden. Eine andere Variante: Angreifer richteten speziell präparierte Webseiten ein und lockten Nutzer anschließend mit Hilfe von Spam-Mails zum Besuch an. Heute findet die Verbreitung von Schadprogrammen mittels Drive-By-Exploits fast ausschließlich über legitime Webseiten statt.

Angreifer manipulieren täglich mehrere tausend Webseiten weltweit und schleusen dort schädlichen Code ein, der zu Drive-By-Exploits führt. Diese Kompromittierung der Webpräsenzen erfolgt meist über gestohlene FTP-Zugangsdaten zu den Webservern, die zuvor mittels Schadsoftware auf den PCs der Webseiten-Betreiber ausgespäht wurden. Von Analysten werden im Rahmen von Ermittlungen auf den Servern der Angreifer regelmäßig Listen mit 30.000 und mehr gestohlenen Zugangsdaten zu FTP-Servern gefunden. Aber auch Sicherheitslücken in Content-Management-Systemen und anderer Server-Software werden von Angreifern für ihre Manipulationen ausgenutzt.

Infektionen auch ohne Mausklick

CERT-Bund, das Computer Emergency Response Team der Bundesverwaltung, erlangt derzeit wöchentlich aus verschiedenen Quellen Kenntnis von mehr als 20 in Deutschland gehosteten Webpräsenzen, die von Angreifern manipuliert wurden und zu Drive-By-Exploits führen. Dies stellt jedoch nur die Spitze des Eisbergs dar, da das BSI nicht aktiv nach kompromittierten Webseiten sucht. Die zuständigen Webseiten-Betreiber werden von CERT-Bund aufgefordert, den eingeschleusten schädlichen Code zu entfernen sowie die von den Angreifern ausgenutzten Schwachstellen zu beheben. Auch beim Besuch von als vertrauenswürdig anzusehenden Webseiten besteht die Gefahr einer Infektion des PCs, und zwar über speziell manipulierte Werbebanner. Angreifer kompromittieren regelmäßig Server-Anwendungen von Marketing-Dienstleistern, so dass mit den Werbebannern schädlicher Code ausgeliefert wird, der zu Drive-By-Exploits führt. Dabei ist nicht einmal das Anklicken des Werbebanners zur Aktivierung des schädlichen Codes erforderlich. Allein die Einblendung des manipulierten Banners auf einer Webseite reicht aus, um die automatisierte Ausnutzung von Schwachstellen auf dem Nutzer-PC zu starten. CERT-Bund hat im Jahr 2010 mehr als 100 Betreiber von Werbebanner-Servern in Deutschland über entsprechende Manipulationen informiert. Die schädlichen Banner wurden unter anderem auf den Webpräsenzen von bekannten Unternehmen, populären Online-Magazinen und TV-/Radio-Sendern eingeblendet.

Exploit-Kits: schädliche Softwarepakete

Der von Angreifern eingeschleuste schädliche Code zielt üblicherweise nicht nur auf die Ausnutzung einer einzelnen Sicherheitslücke ab. Meistens führt er zu einem so genannten Exploit-Kit. Ein Exploit-Kit (auch „Exploit Pack“ genannt) ist ein Softwarepaket, das die Ausnutzung von Schwachstellen auf Nutzer-PCs mittels Drive-By-Exploits und die anschließende Infektion mit einem Schadprogramm automatisiert. Neben einer Sammlung von Exploits für verschiedene (typischerweise mehr als zehn) Schwachstellen enthält es eine webbasierte Managementoberfläche zur komfortablen Konfiguration und Ausgabe von Statistiken. Exploit-Kits werden unter Cyber-Kriminellen je nach Anzahl und Aktualität der enthaltenen Exploits für ca. 400 bis 2.000 US-Dollar gehandelt. Für die Installation und den Betrieb eines Exploit-Kits sind üblicherweise keine tief gehenden technischen Kenntnisse erforderlich.

Ausgenutzte Schwachstellen

Im Fokus der Angreifer standen in den letzten Monaten in erster Linie Schwachstellen in veralteten Versionen der weit verbreiteten Anwendungsprogramme Adobe Reader und Flash sowie in der Java-Laufzeitumgebung. Aber auch bei der Ausnutzung von zum Teil schon seit Jahren bekannten Sicherheitslücken im Internet Explorer und im Windows-Betriebssystem sind Exploit-Kits noch recht erfolgreich. Denn auf vielen PCs sind die verfügbaren Sicherheitsupdates, die die Lücken schließen, noch nicht installiert.

Besonders kritisch wird es, wenn „Zero-Day-Exploits" zum Einsatz kommen, also Schwachstellen ausgenutzt werden, für die noch kein Sicherheitsupdate des Herstellers der verwundbaren Software zur Verfügung steht.

Fazit:

Ob eine Webseite manipuliert wurde und zu Drive-By-Exploits führt, ist für den Besucher üblicherweise nicht einfach erkennbar. Die Ausnutzung von Schwachstellen und die anschließende Installation von Schadsoftware auf dem PC erfolgt unbemerkt und ohne weitere Nutzerinteraktion. Die zeitnahe Installation aller verfügbaren Sicherheitsupdates für Betriebssystem und Anwendungssoftware ist deshalb zur Abwehr von Infektionen unbedingt erforderlich. Ein Virenschutzprogramm allein bietet auf Grund der Masse der täglich neu verbreiteten Schadprogrammvarianten keinen ausreichenden Schutz.

3 Botnetze

Botnetze

Ein Botnetz ist ein Zusammenschluss infizierter PCs, die von einem Angreifer ferngesteuert werden. Er kann auf diese Weise beispielsweise unbemerkt Spam versenden, Tastatureingaben ausspähen oder Angriffe auf andere Systeme vornehmen, etwa Webserver oder ganze Netze. Ist ein PC erst einmal – auf welche Weise auch immer – infiziert, kann ihn ein Angreifer als Teil eines Botnetzes für vielfältige Zwecke missbrauchen.

Die Bedrohung durch Botnetze hat in den vergangenen zwei Jahren weiterhin massiv zugenommen. Dazu trägt auch die zunehmende Infektionsgefahr durch Drive-By-Exploits bei. Außerdem werden Botnetze mittlerweile professionell vermietet, und ihre „Kunden" nutzen sie zum Beispiel, um Vergeltung auszuüben, Wettbewerbsvorteile zu erlangen und für kriminelle Zwecke wie etwa Erpressung. Hinzu kommen politisch oder religiös motivierte Angriffe. Im Jahr 2010 trat zunehmend ein weiterer Trend auf: Beim so genannten „Hacktivismus", einer Mischform von Hacking und Aktivismus, stellen Internet-Nutzer ihre PCs freiwillig zur Verfügung, um Angriffe, beispielweise DDoS-Angriffe, auf Unternehmen durchzuführen. Auf diese Weise kann sich ebenfalls ein Botnetz bilden.

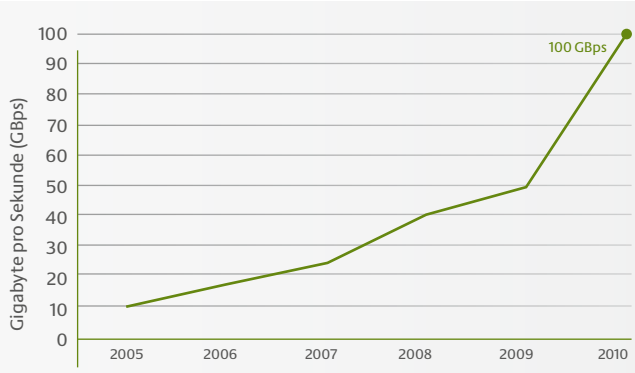
Botnetz-Betreiber können potenziell eine zunehmende Anzahl von PCs infizieren, denn immer mehr Anwender verfügen über einen Breitband-Internet-Anschluss und haben ihre Computer rund um die Uhr ans Internet angeschlossen. Dadurch steigt auch die Intensität der Cyber-Attacken – nach Einschätzungen des BSI überschreitet sie bereits jetzt die Bandbreite der Leistungen einzelner Provider, was zu Netzausfällen führen kann.

Häufig bemerken Anwender nicht, dass ihr PC Teil eines Botnetzes ist, da die Schadfunktionen nur im Hintergrund ablaufen. Die Analyse eines Sicherheitsunternehmens, bei der weltweit 100 Millionen auffällig gewordene IP-Adressen beobachtet wurden, bestätigt dies. Sie zeigt, dass 80 Prozent der IP-Adressen, hinter denen infizierte PCs stehen, mehr als einen Monat und 50 Prozent sogar mehr als 300 Tage in der Statistik auftauchten.[3] Ein Grund dafür ist, dass Bot-Software teilweise Antiviren-Software deaktiviert, um nicht entdeckt zu werden. Fehlende oder veraltete Antiviren-Software auf den Rechnern der Anwender verstärkt das Problem. Erkannt wird die Infektion daher häufig erst, wenn der Anwender von seinem Provider darüber informiert wird. Auch die Anzahl an Mehrfachinfektionen mit Bot-Software hat zugenommen. Dies bestätigt eine Analyse, bei der in 35 Prozent der Fälle eine Mehrfachinfektion beobachtet wurde.[4]

Fazit:

Das „Geschäftsmodell" Botnetze hat sich für Kriminelle bewährt und wird daher auch in den nächsten Jahren weiteren Zuwachs erfahren. Das Aufkommen von „Hacktivismus" zeigt, dass Angriffe auch zunehmend durchgeführt werden, um politische Ansichten auszudrücken und sich so Gehör zu verschaffen.

Intensität von DDoS-Angriffen



Quelle: Arbor Networks

Abb. 5: Bandbreitenzuwachs bei DDos-Angriffen [9]

Anti-Botnetz-Initiative entzieht Infektionen nachhaltig den Boden

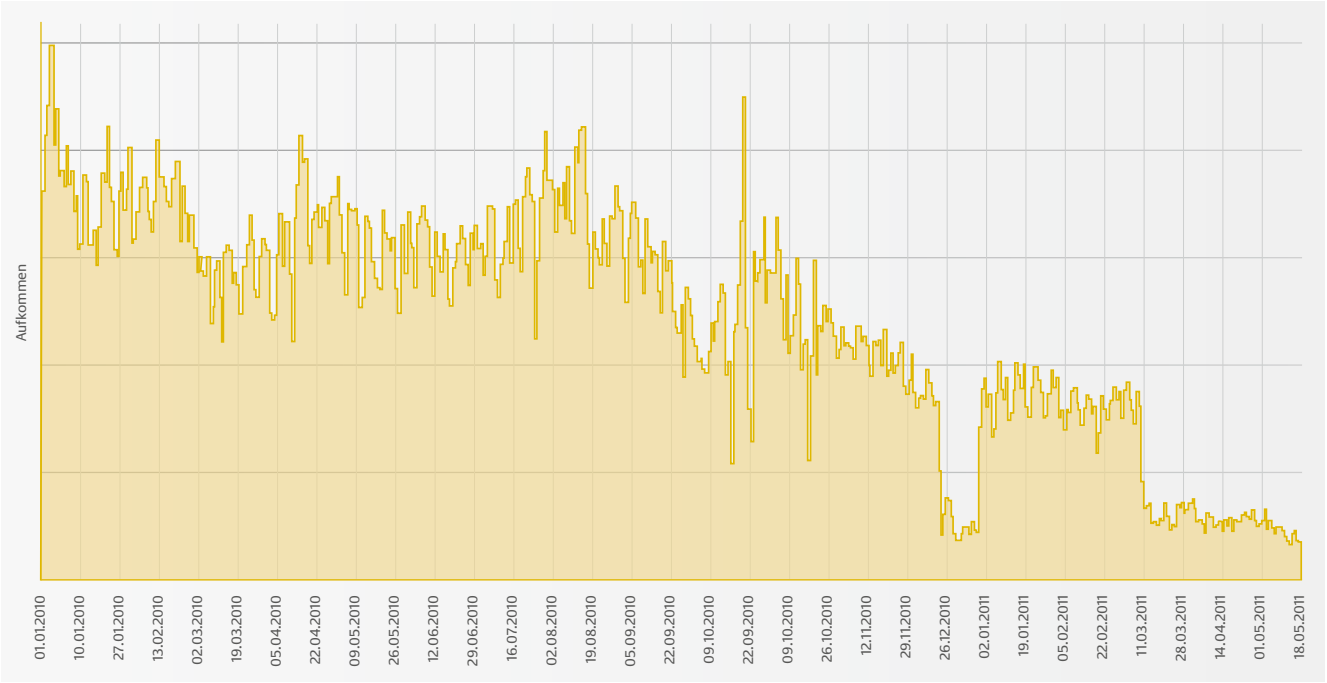
Bei Botnetzen, die Spam-E-Mails versenden, gehört Deutschland nach Analysen des BSI im Ländervergleich zu den Top 5. Das BSI unterstützt deshalb das Anti-Botnet-Beratungszentrum des eco-Verbands der deutschen Internetwirtschaft e.V. Die Initiative wird vom Bundesministerium des Innern (BMI) durch eine Anschubfinanzierung aus Mitteln des IT-Investitionsprogramms gefördert. Sie hilft Anwendern dabei, Bot-Infektionen von ihren Rechnern zu entfernen. Diese Initiative, die am 15. September 2010 offiziell gestartet ist, schafft mehr Sicherheit für den Endnutzer und soll Botnetzen, die in beziehungsweise aus Deutschland heraus agieren, in weiten Teilen nachhaltig den Boden entziehen. Dafür sieht die Initiative zunächst die Identifizierung infizierter Rechner vor. Dies geschieht durch den Internet Service Provider (ISP) mittels so genannter „Honeypots“ und „Spamtraps“. Die Honeypot-Systeme befinden sich im Netzbereich des Providers und werden von dem infizierten Rechner angegriffen. Die „Spamtraps“ der Provider empfangen Spam-E-Mails. Anschließend werden die identifizierten Nutzer über die Infektion ihres Rechners durch die beteiligten ISPs informiert. Um die Infektion zu beseitigen, erhalten sie auf der zentralen Webseite www.botfrei.de Hilfen in Form von Informationen und Tools. Anwender, die weitere Hilfe benötigen, erhalten über den ISP die Möglichkeit, die telefonische Beratungshotline des Anti-Botnet-Beratungszentrums zu nutzen. Seit dem Projektstart am 15. September bis zum 30. April 2011 nutzten bereits über 994.000 Besucher die Angebote der Webseite. In dieser Zeit haben sie die DE-Cleaner – spezielle Tools, um die Botsoftware vom Rechner zu entfernen – bereits mehr als 522.000 Mal eingesetzt. Die beteiligten ISPs haben mehr als 200.000 Kunden über die Infektion ihres Rechners benachrichtigt.

4 Spam

Die Anzahl unerwünschter E-Mails (Spam) ist im Vergleich zum Rekordjahr 2008 gesunken. Der Spam-Anteil bleibt aber mit 96,1 Prozent im Jahr 2010 weiterhin beträchtlich. Zugleich scheint der Versand gezielter zu erfolgen. So wächst beispielsweise jener Anteil von Spam-E-Mails, die von internationalen Botnetzen in deutscher Sprache speziell an deutsche E-Mail-Empfänger versendet werden.

Der überwiegende Teil von Spam wird von Botnetzwerken versendet. Das BSI konnte in einer einzigen Stunde einzelne Spam-Wellen mit über 100.000 unterschiedlichen Quellen (einmal vorhandene IP-Adressen der sendenden Systeme) beobachten. Das Rustock-Botnetz scheint hier der wichtigste Spam-Versender des letzten Jahres zu sein. Bei seiner zweiwöchigen Sendepause Ende 2010 und nach der Abschaltung seiner Steuer-Rechner in den USA ging das Spamvolumen in Deutschland sprunghaft um fast 75 Prozent zurück, wie die folgende Grafik zeigt:

Spamentwicklung in Deutschland



Quelle: BSI

Abb. 6: Entwicklung des Spamaufkommens in Deutschland seit Januar 2010 [7]

Spamversand über private PCs

Der Spamversand weist sowohl im Tagesablauf als auch im Wochenverlauf Regelmäßigkeiten auf. Besonders interessant ist zudem die länderspezifische Betrachtung der Quellen.

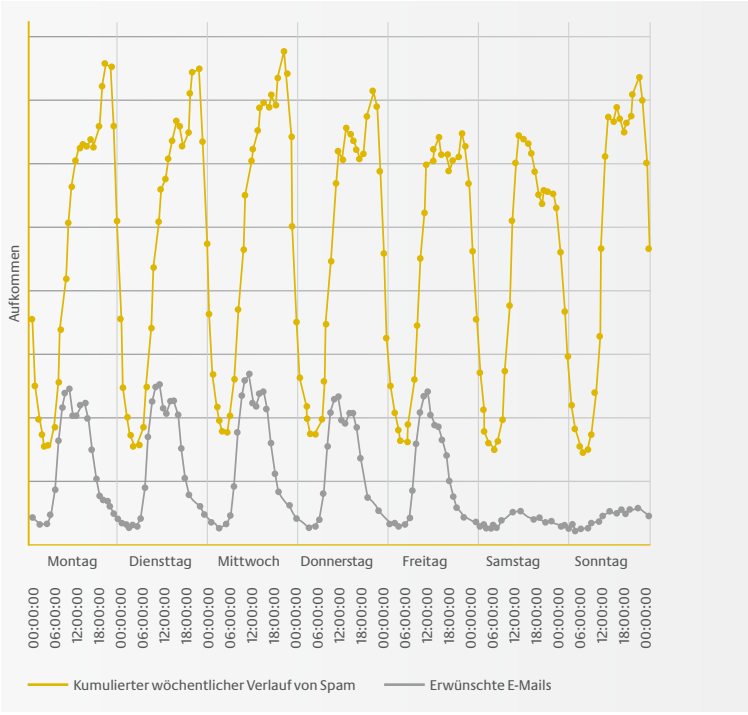
Die folgende Abbildung zeigt in einem über mehrere Monate kumulierten Wochenverlauf stundengenau den Versand von Spam- und Nutzmails aus Deutschland, gemessen am E-Mail-Frühwarnsystem des BSI.

Nach Erkenntnissen des BSI werden in Deutschland die meisten Spam-Nachrichten von kompromittierten privaten PCs versendet. Diese werden am Nachmittag wahrscheinlich von Schülern, in den Abendstunden dagegen – also nach Feierabend – verstärkt von Erwachsenen in Betrieb genommen. Freitag- und Samstagabend werden hingegen weniger der infizierten PCs betrieben – an diesen Tagen stehen vermutlich andere Freizeitaktivitäten im Vordergrund. Im internationalen Vergleich fällt auf, dass es Länder gibt, in denen das Tagesmaximum in die zeitzonenspezifische Arbeitszeit fällt und sich in den Abendstunden und am Wochenende stark reduziert. Hier scheint der Versand vor allem über Arbeitsplatz-PCs zu erfolgen.

In der Länderverteilung der Spam versendenden Länder belegt Deutschland mit 5,77 Prozent im Jahr 2010 den vierten Platz nach den USA (9,32 Prozent), Brasilien (8,36 Prozent) und Indien (7,28 Prozent). Der deutsche Anteil nimmt im Verlauf des Jahres ab. Die Angaben beziehen sich auf die Spamverteilung in der Bundesrepublik.

Das BSI erwartet, dass Deutschland im Jahr 2011 als Spamquelle von einigen Ländern überholt werden wird.

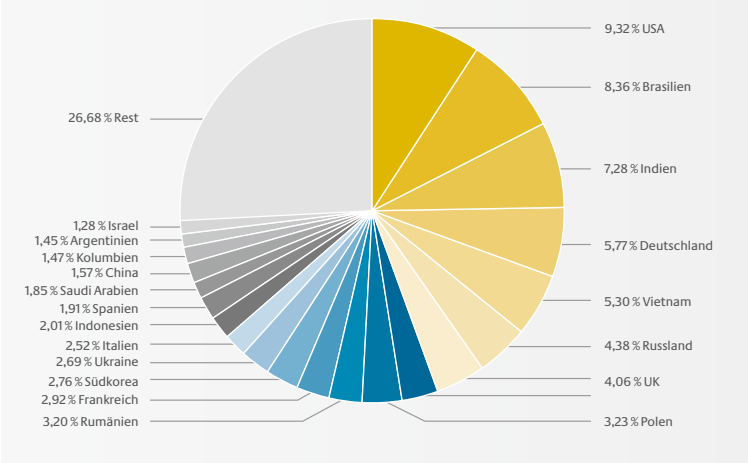
Spamversand im Wochenverlauf



Quelle: BSI

Abb. 7: Kumulierter wöchentlicher Versand von Spam und erwünschten E-Mails aus Deutschland [7]

Spamverteilung nach Ländern



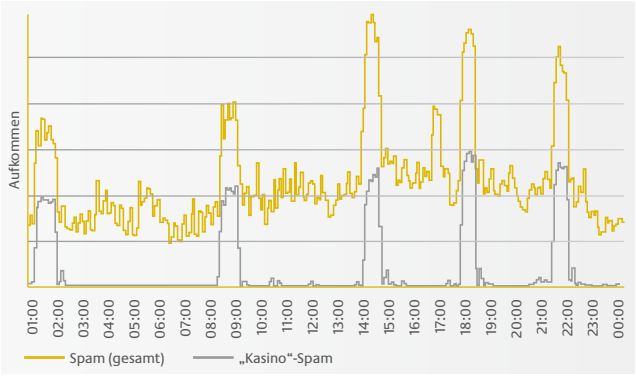
Quelle: BSI

Abb. 8: Spamverteilung in der Bundesrepublik nach Ursprungsländern in 2010 [7]

Deutschsprachige Kasino-Spamwellen aus tausend Quellen

Eine der markantesten dauerhaften Spam-Aktionen, die vom BSI bereits seit Mai 2009 beobachtet wird, ist die deutschsprachige „Kasino-Werbung“. Sie tritt in circa einstündigen Versand-Wellen auf, die das Spamaufkommen um mehr als 100 Prozent anheben. Als Versender konnten mehrere tausend Quellen pro Stunde aus fast allen Ländern der Welt identifiziert werden – vor allem aus Brasilien, gefolgt von Vietnam, Indien, Indonesien, China und Deutschland. Sie gehören sehr wahrscheinlich zu dem Botnetz „Maazben“. Aus den Zeitverläufen kann geschlossen werden, dass große Teile dieses Botnetzes sich simultan auf eine Länderdomäne und die dazugehörige Sprache konzentrieren.

„Kasino“-Spam



Quelle: BSI

Abb. 9: „Kasino“-Wellen und Gesamt-Spamaufkommen im beispielhaften Tagesverlauf [7]

Anwerbungen von Internet-Nutzern für kriminelle Zwecke

Seit März 2010 ist eine Spam-Welle zu beobachten, mit der „Arbeitskräfte“ angeworben werden sollen. Diese „Money-Mules“ oder „Agenten“ werden dann zum Weiterleiten von illegal erworbenen Gütern oder Geldern eingesetzt. Um die Glaubwürdigkeit dieses Angebots zu steigern, wird in der Kampagne oft die Bundesagentur für Arbeit (BA) als Adressenlieferant genannt. Als Versender dieser Spams konnten pro Stunde mehrere tausend unterschiedliche Quellen aus fast allen Ländern der Welt lokalisiert werden – vor allem aus Brasilien, gefolgt von Indien, Südkorea, Deutschland und Polen.

Für diese Spam-Variante fand Mitte März 2010 seitens der Angreifer zunächst ein kleiner und anscheinend sehr erfolgreicher Test statt. Von Ende April bis Ende August 2010 gehörte diese Form der E-Mails fest zur deutschen Spamlandschaft. Danach wurde auf die Nennung der BA weitgehend verzichtet. Ende des Jahres erschien eine weitere Welle. Sie ließ direkt im ersten Satz keine Zweifel daran, dass die Anwerbung für kriminelle Zwecke erfolgen sollte: *„Eine Arbeit fur jemanden der sich im Klaren ist, dass falls was schief gehen sollte er im bestenfalls mit einer Bewahrungsstrafe auskommt, im schlimmsten ....“* Dieses Beispiel zeigt, dass die Angreifer nicht davor zurückschrecken, breite Schichten der Bevölkerung in kriminelle Handlungen zu verwickeln. Die Bundesagentur für Arbeit hat direkt nach einer Warnung durch das BSI mehrfach Pressemeldungen zu diesem Thema veröffentlicht.

Fazit:

Zwar nimmt die Gefahr durch überlastete Empfänger-Mail-Infrastrukturen ab. Doch werden die Inhalte krimineller Spams immer überzeugender. Dadurch steigt das Risiko für die Empfänger – beispielsweise durch Medikamentenfälschungen, Spielsucht, (unbewusste) Teilnahme an kriminellen Tätigkeiten, Preisgabe von sensiblen Daten oder durch Schadsoftware. Dieser Trend wird sich in Zukunft fortsetzen.

5 Identitätsdiebstahl und -missbrauch

Identitätsdiebstahl und -missbrauch

In der Informationstechnik wird die Identität einer Person allgemein als eine Datenmenge definiert, die eben diese Person in bestimmten Zusammenhängen von anderen Personen unterscheidet. Das einfachste Beispiel ist ein Benutzername und das zugehörige Passwort. Gelangt jemand unbefugt an diese Daten, so liegt ein Identitätsdiebstahl vor, der oftmals mit einem Identitätsmissbrauch einhergeht. In erster Linie wollen sich die Täter dabei einen finanziellen Vorteil verschaffen, seltener soll eine Person diskreditiert werden.

Identitätsdiebstahl und Identitätsmissbrauch sind keine neuartigen Delikte: Es gab sie schon vor dem Einsatz elektronischer Medien. Dabei waren sich Täter und Opfer jedoch fast immer geografisch relativ nahe, und meist gab es nur wenige Betroffene. Mit der zunehmenden Nutzung des Internets hat sich die Situation jedoch radikal gewandelt: Zwischen Tätern und Opfern gibt es meist keinerlei geografischen Zusammenhang mehr. Zudem kann sich ein Täter mit geringem Aufwand – nämlich durch den Einsatz von Schadprogrammen – die Daten von hunderten oder tausenden Opfern verschaffen. Das haben die Analysen der Datensätze, die von Tätern erbeutet wurden, gezeigt.

Schadprogramme stehlen persönliche Daten

Für einen Identitätsdiebstahl werden Schadprogramme eingesetzt, die die gestohlenen Daten auf von den Tätern kontrollierte Server im Internet übertragen. Die auf diesen so genannten Dropzones liegenden Daten werden dann in der Folge für den eigentlichen Identitätsmissbrauch eingesetzt. Gelegentlich können Daten, die von Schadprogrammen auf die Dropzones übertragen werden, abgefangen werden. Gelingt dies, werden die Inhaber der gestohlenen Identitäten meist über die jeweiligen Betreiber der betroffenen Internetangebote geschützt, etwa durch einen präventiven Passwortwechsel oder die vorübergehende Deaktivierung des Zugangs.

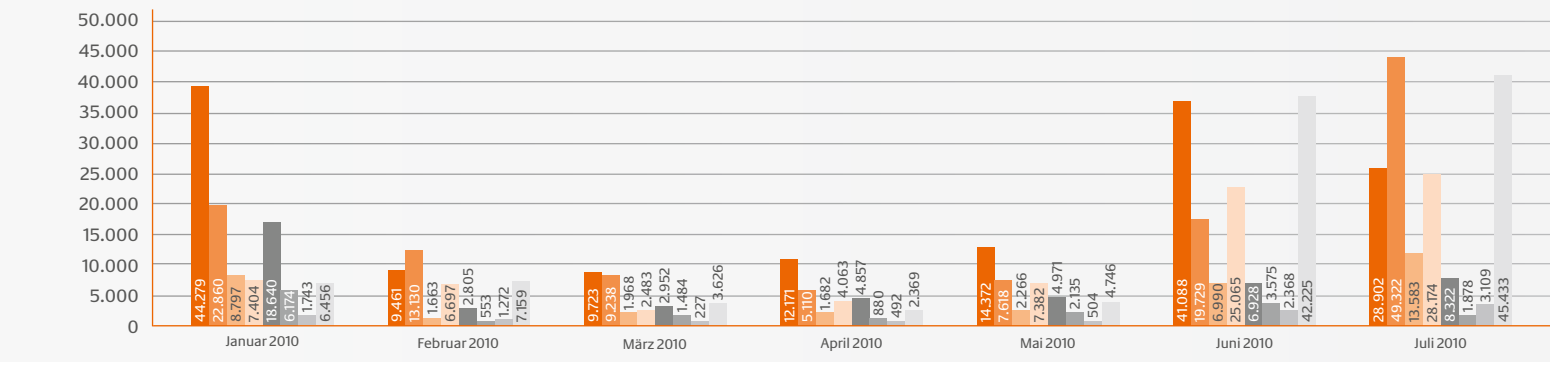
Im Jahr 2010 konnten Daten aus etwa 200 Dropzones analysiert werden. Dabei sind für das BSI insbesondere Datensätze mit einem unmittelbaren Bezug zu Deutschland, wie er sich zum Beispiel aus der Domainendung „de“ ergibt, von Interesse.

Insbesondere bei Webmailern und Handelsplattformen verbreitet

Die Auswertung exemplarischer Dropzone-Datensätze aus dem Jahr 2010 zeigt, dass es den Tätern insbesondere gelang, an Zugangsdaten für deutsche Anbieter von Webmail-Diensten sowie für weit verbreitete Handelsplattformen zu gelangen. Diese Identitäten lassen sich beim anschließenden Missbrauch zwar nur mittelbar zu Geld machen, bergen aber dennoch erhebliches Schadenspotenzial. Das E-Mail-Konto stellt bei vielen Nutzern den zentralen Vertrauensanker für viele andere Aktivitäten im Internet dar, sodass darüber leicht weitere Zugangsdaten erlangt werden können. Gestohlene Identitäten für Handelsplattformen bieten eine ideale Grundlage für betrügerische Kauf- und Verkaufstransaktionen.

Unmittelbar auszunutzen sind hingegen Zugangsdaten zum Online-Banking. Im Jahr 2010 konnten in den untersuchten Dropzones ca. 86.000 entsprechende Identitäten gefunden werden. Zwar erlauben diese Zugangs-

Dropzone-Datensätze



Quelle: BSI

Abb. 10: Dropzone-Datensätze 2010 aus ca. 200 Dropzones mit direktem Bezug zu .de-Domains [7]

daten allein noch keine Durchführung einer Transaktion. Da allerdings auf den angegriffenen Zielsystemen in den meisten Fällen noch Schadprogramme aktiv sind, können oftmals auch die weiteren Schutzmechanismen der Banken, etwa TAN-Verfahren, von Angreifern überwunden werden.

Private PCs werden mit Trojanischen Pferden durchsucht

Die Täter nutzen mittlerweile fast ausschließlich „Trojanische Pferde", die unbemerkt auf den Rechnern der Opfer platziert werden. Auf diese Weise lesen sie die Eingaben des Computerbesitzers bei berechtigten Anmeldevorgängen oder Transaktionen direkt mit, oder sie durchsuchen die Dateien auf dem Rechner nach bestimmten Stichwörtern. Anschließend erfolgt die Übermittlung der Daten an die Dropzones im Internet.

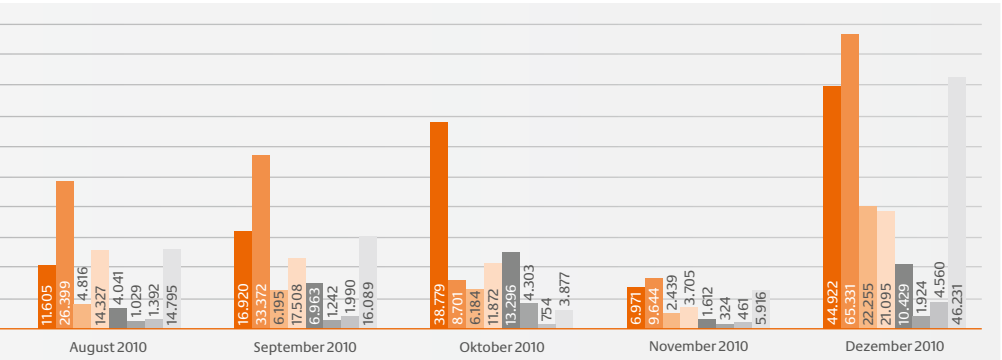
Das klassische Phishing – also das Locken auf beispielsweise gefälschte Bank-Webseiten mit Aufforderung zur Dateneingabe – ist hingegen praktisch nicht mehr feststellbar. Der verstärkte Einsatz von leistungsfähigen Trojanischen Pferden führt jedoch dazu, dass die Fallzahlen – und damit auch die Schadenshöhen – gegenüber den letzten Jahren wieder gestiegen sind.

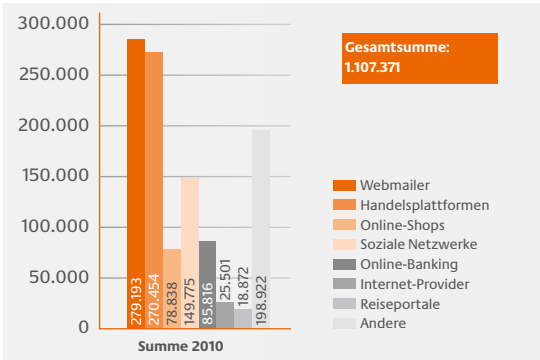
Die Täter gehen heute sehr arbeitsteilig und orchestriert vor: Eine erste Gruppe erstellt die Schadprogramme, zum Beispiel „Trojanische Pferde". Die nächste Gruppe sorgt für die Verteilung und den Einsatz der Schadsoftware im Internet, während eine weitere Gruppe die ausgespähten Daten aus den Dropzones einsammelt und für den anschließenden Identitätsmissbrauch aufbereitet. Diese Daten werden dann von den weiteren Tätern kriminell eingesetzt.

Da eine direkte Überweisung ins Ausland aufgrund von Sicherheitsmaßnahmen der Banken und Angebotsanbieter nicht ohne weiteres möglich ist, werden so genannte Finanzagenten mit inländischen Konten zwischengeschaltet. Auch deren Gewinnung und Betreuung, unter anderem durch Spam-Versand (vgl. Kapitel 4), ist ausgefeilt organisiert.

Fazit:

Identitätsdiebstahl und Identitätsmissbrauch haben sich als ein kriminelles Betätigungsfeld etabliert, das mit hoch professionellen Strukturen bearbeitet wird. Das klassische Phishing ist in den vergangenen Jahren immer weniger geworden und kaum noch feststellbar. Stattdessen nutzen die Angreifer fast ausschließlich Trojanische Pferde.





6 Schadprogramme

Im Lagebericht 2009 wurde festgestellt, dass die Anzahl bösartiger Programme stetig zunimmt, ihre Herstellung immer einfacher wird und die Angriffe zunehmend gezielt verlaufen. Diese Trends haben sich seitdem verstärkt:

Detektion von Schadprogrammen deutlich schwieriger

Die Anzahl neuer Schadprogramme nimmt weiterhin sehr stark zu. Alle ein bis zwei Sekunden entsteht ein neues. Schadprogramme werden aber nicht mehr wahllos in großen Wellen im Internet gestreut. Gab es früher regelmäßig mehrere tausend oder sogar hunderttausend Opfer, die von demselben Schadprogramm heimgesucht wurden, sind heute oft nur weniger als 20 Rechner weltweit betroffen. Besucher einer manipulierten Webseite, die per Drive-By-Download infiziert werden, erhalten zum Teil sogar einen individuellen Schadcode. Besonders problematisch sind dabei Schadprogramme, die nur auf dem Rechner lauffähig sind, den sie zuerst infiziert haben, da sie sich bei einer Analyse völlig unauffällig verhalten.

Ein Schadprogramm wurde früher über viele Monate aktiv genutzt. Heute wird ein bestimmtes Schadprogramm nur wenige Tage verwendet, bevor es durch eine neue Variante, die nicht mehr von Viren-Schutzprogrammen gefunden wird, ersetzt wird.

Aus diesen Trends folgt unmittelbar, dass die übliche Detektion von Schadprogrammen anhand von Signaturen und Prüfsummen immer schwieriger wird. Hersteller von Viren-Schutzprogrammen haben große Probleme, die Vielzahl unterschiedlicher Schadprogramme zu orten und Erkennungssignaturen zu erstellen.

Es gibt zwei Hauptursachen für die Flut neuer Schadprogramme: Exploit-Kits und Virenbaukästen sind für jeden verfügbar, werden innerhalb weniger Tage um neu veröffentlichte Schwachstellen und Angriffsmethoden erweitert und können auch von semiprofessionellen Angreifern leicht bedient werden. Zum anderen gibt es sehr effiziente Techniken, um aus einem bestimmten Schadprogramm automatisiert tausend neue Varianten mit kleinen Unterschieden und unterschiedlichen Prüfsummen zu erzeugen.

Verbreitung von Schadsoftware hauptsächlich über Drive-By-Downloads

Die Verbreitung von Schadsoftware über E-Mails nimmt ab. Das BSI geht davon aus, dass die meisten Schadprogramme inzwischen über Drive-By-Downloads verteilt werden. Immer mehr Schadprogramme, die einen Rechner über das Internet infiziert haben, verbreiten sich danach auch über USB-Sticks oder interne Netzwerke weiter. Immer häufiger werden manipulierte Microsoft Office- oder Adobe PDF-Dokumente verwendet. Zudem sind Schadprogramme für mobile Geräte auf dem Vormarsch: Ein Überspringen von Schadcode zwischen PC und mobilem Gerät bei der Datenübertragung ist inzwischen technisch kein Problem mehr, auch wenn derartige Fälle in der Praxis noch selten beobachtet werden.

Ein Grund für den Rückgang E-Mail-basierter Angriffe liegt in einer stetigen Verbesserung der Spam-Filter, die als Nebeneffekt die Zustellung infizierter Mails verhindern.

Infizierte E-Mails im Regierungsnetz

Insgesamt wird die Gesamtzahl infizierter E-Mails im Regierungsnetz immer geringer. Gleichzeitig entdeckt das BSI aber immer mehr schädliche E-Mails, die von Virenscannern nicht erkannt wurden. Zurzeit detektiert das BSI etwa vier bis fünf zielgerichtete Angriffe pro Tag.[2]

Im Jahr 2004 wurden in jedem Monat mehr als 100.000 infizierte E-Mails von einem Standard-Virenscanner geblockt – viele davon mit demselben Schadprogramm. Im Durchschnitt gab es im Jahr 2004 1,6 Millionen schädliche E-Mails pro Monat. In den letzten fünf Jahren gab es nur noch sechs Monate mit mehr als 100.000 infizierten E-Mails. Relativ gesehen ist der Anteil der vom Virenscanner detektierten schädlichen E-Mails noch stärker zurückgegangen, da 2010 circa viermal so viele Mails empfangen wurden wie in 2004. Entwarnung? Leider nicht. Waren infizierte E-Mails 2004 relativ leicht mit Viren-Schutzprogrammen zu detektieren, entdeckt das BSI mit eigenen Erkennungssystemen immer mehr schädliche E-Mails, die vom Virenscanner nicht erkannt wurden. Diese Zahlen verdeutlichen die Vorteile zentraler Schutzmaßnahmen im Regierungsnetz. Die gesamte Bundesverwaltung profitiert so von dem hohen technologischen und personellen Aufwand, den das BSI zum Schutz des Regierungsnetzes betreibt.

Schutzmaßnahmen verbesserungswürdig

Der Wettlauf zwischen den Autoren von Schadprogrammen und Herstellern von Schutzprogrammen verläuft in immer rasanterem Tempo, was nicht ohne Folgen bleibt. Nach einer internen Untersuchung des BSI ist insbesondere die Erkennungsrate von Dokumenten mit eingebetteter Schadfunktion durch Virenscanner stark verbesserungsbedürftig. Im On-Demand-Modus (also ohne die Datei auszuführen) wurden durchschnittlich weniger als die Hälfte der bösartigen Dokumente erkannt. Erst durch eine Kombination von mindestens drei unterschiedlichen Virenscannern konnten über 90 Prozent der schädlichen Dokumente identifiziert werden. On-Access-Virenscanner, die beim Öffnen einer Datei zusätzliche Detektionsverfahren nutzen, schneiden hier besser ab. Viren-Schutzprogramme auf Arbeitsplatz-PCs sind daher denen an Gateways, die nur im On-Demand-Modus arbeiten, deutlich überlegen – wenn alle verhaltensbasierten und heuristischen Detektionsverfahren aktiviert werden.

Welche Maßnahmen helfen neben dem Einsatz von Viren-Schutzprogrammen, die in vielen Szenarien keine ausreichende Sicherheit mehr bieten können? Gegen Drive-By-Downloads beim Surfen kann man sich mit Virtualisierungstechniken schützen. Der Browser wird dabei zum Beispiel in einer virtuellen Umgebung gekapselt und so wirksam vom Rest des Rechners und vom Intranet getrennt. Auf diese Weise werden zumindest Datenverlust oder Sabotagehandlungen durch Schadprogramme wirksam verhindert. Gegen die Verbreitung von Schadsoftware über USB-Sticks werden vermehrt

[2] Das BSI spricht von einer „gezielten" Attacke, wenn der Angreifer sie individuell auf eine bestimmte Person zuschneidet und zur Tarnung einen hohen Aufwand an Social Engineering betreibt. Die verwendeten Schadprogramme werden dabei so lange verändert bis gängige Virenschutzprogramme sie nicht mehr erkennen.

Programme zur Kontrolle der Rechnerschnittstellen eingesetzt, deren Verwendung mit teils erheblichen Komfort- und Funktionseinbußen einhergeht. Gegen Schadrogramme in E-Mails gibt es außer der Verwendung mehrerer verschiedener Viren-Schutzprogramme kaum zusätzliche Maßnahmen. E-Mails sind so stark in typische Arbeitsprozesse eingebunden, dass eine Virtualisierung der E-Mail-Programme nicht infrage kommt. Die IT-Sicherheitsindustrie hat auf diese Situation reagiert und bietet gemanagete Sicherheitsdienstleistungen wie einen zentralen E-Mail-Scan oder Spamabwehr an. Für viele Unternehmen – aber auch den Bürger – werden Sicherheitsdienstleistungen durch spezialisierte Unternehmen oder Provider zukünftig eine interessante Alternative zum Eigenbetrieb von Schutzsoftware sein. Weiterhin problematisch ist die um sich greifende Verwendung mobiler Geräte zur Verarbeitung und Speicherung vertraulicher Informationen. Mobile Geräte sind häufig schlecht geschützt. Eine engere Kooperation der Hersteller von mobilen Geräten, Betriebssystemen und Schutzsoftware ist hier dringend notwendig.

Fazit:

Große Schadprogramm-Wellen wie Sasser oder Loveletter sind nicht mehr zu beobachten. Ein typisches Schadprogramm hat eine Einsatzdauer von wenigen Tagen und wird nur gegen einen kleinen Opferkreis eingesetzt. Aufgrund dieser Individualisierung von Angriffen steigt die Anzahl von Schadprogrammen mit unterschiedlicher Prüfsumme weiter ungebremst. Signaturbasierte Viren-Schutzprogramme bieten daher keinen zuverlässigen Schutz mehr und müssen durch eine Kombination anderer Verfahren ergänzt werden. Gezielte Angriffe zu Sabotage- und Spionagezwecken nahmen im Berichtszeitraum stark zu und wurden mit einer bislang nicht gekannten Professionalität durchgeführt. Sorge bereitet dem BSI die um sich greifende Verwendung mobiler Geräte zum Lesen und Schreiben von E-Mails, da diese mangels geeigneter Schutzprogramme häufig nur schlecht geschützt sind.

7 Stuxnet

Stuxnet

In den letzten Monaten stand das Schadprogramm Stuxnet, das im Juli 2010 entdeckt wurde, im besonderen Fokus der Öffentlichkeit. Dieses Beispiel zeigt sehr deutlich die professionelle Arbeitsweise der Angreifer und die Gefährlichkeit gezielter Angriffe auf Industrieanlagen. Es handelt sich dabei um eine Schadsoftware, die mit enormem Aufwand programmiert wurde, um besondere Schutzmechanismen zu umgehen. Dadurch ist sie in der Lage, industrielle Prozesssteuerungssysteme anzugreifen. Die erfolgten Angriffe zielten ausschließlich auf Prozesssteuerungsrechner, auf denen die SCADA-Software „WinCC“ von Siemens verwendet wird. Mit Hilfe der Schadsoftware konnte eine ganz bestimmte Anlagenkonstellation filigran sabotiert werden. Weltweit beobachteten die Hersteller von Antiviren-Software mehrere hunderttausend erfolgreicher Infektionen verschiedenster PCs, alle ohne Schadwirkung, vermutlich als Kollateral-Infektionen. Die von Siemens-Kunden aus dem industriellen Umfeld bestätigten 22 Infektionen führten in keinem Fall zu Auswirkungen auf die Industrieanlagen. Inzwischen sind die von Stuxnet ausgenutzten Schwachstellen im Windows-Betriebssystem geschlossen worden.

Nachdem IT-Angriffe auf Prozesssteuerungssysteme lange Zeit lediglich in Fachkreisen diskutiert wurden, ist durch Stuxnet die reale Bedrohung nun eindrucksvoll bewiesen worden. Das Schadprogramm zeichnet sich durch herausragende Infektionsmechanismen aus und richtet sich im Gegensatz zu den meisten Trojanischen Pferden nicht gegen „normale“ PCs, sondern gegen Prozesssteuerungsanlagen in der Industrie. Diese sind die „Gehirne und Nervenbahnen“ für viele Abläufe: Sie messen, steuern und regeln komplexe Anlagen wie Raffinerien, Pipelines, Stromnetze oder Backstraßen, Fertigungsbänder und vieles mehr. Mit der Spekulation über mögliche Angriffsziele im Bereich der Atomwirtschaft wurde das Thema Stuxnet in vielen Medien aufgegriffen und diskutiert.

Stuxnet ist unter dem Strich weniger in seiner Eigenschaft als konkrete Schadsoftware alarmierend – wichtig ist vielmehr der nun vorliegende Nachweis über die Möglichkeit von Angriffen solcher Qualität. Es gibt demnach Täter, die weder Kosten noch Mühen scheuen, um aus ihrer Sicht sehr wichtige Ziele mittels der IT anzugreifen und möglichst unbemerkt zu sabotieren. Wurden bislang Angriffe auf Kritische Infrastrukturen und ihre Prozesssteuerungssysteme wegen der vermeintlich geringen Wahrscheinlichkeit häufig als Restrisiko akzeptiert, so gilt es nun, dieses Risiko neu zu bewerten.

Prozesssteuerungen von anderen Netzen trennen

Stuxnet war für ein bestimmtes Ziel programmiert und exakt darauf abgestimmt. Ein qualitativ ähnlich hochwertiger Angriff auf ein anderes Ziel würde erneut Programmieraufwand in vergleichbarem Umfang erfordern. Dennoch besteht erhebliche Gefahr, dass Stuxnet nur die bekannt gewordene „Spitze eines Eisbergs“ ist und ähnlich konzipierte Angriffe folgen könnten. Es ist nicht auszuschließen, dass heute vergleichbare Schadprogramme sowohl für Prozesssteuerungssysteme anderer Betreiber und Hersteller als auch für andere kritische Informationsinfrastrukturen mit noch ebenso unbekannten Infektionswegen und hochkomplexen Schadfunktionen programmiert und eingesetzt werden. Neben solchen hochspezialisierten und gezielten Angriffen besteht auch die Gefahr von Trittbrettfahrern, die versuchen könnten, mit deutlich geringerem Aufwand Schaden in Prozesssteuerungen anzurichten. Daher gilt es, diese Systeme möglichst strikt von sonstigen Netzen zu isolieren und zwingend notwendige Schnittstellen bestmöglich zu schützen und zu überwachen.
In einigen Fällen hat das BSI nachgewiesen, dass Prozesssteuerungssysteme schon direkt über das Internet sichtbar und erreichbar sind. Und was sichtbar ist, kann angegriffen werden.

Fazit:

Durch Stuxnet wird deutlich, dass die gesamte Sicherheitskonzeption von Systemen zur Prozesssteuerung dringlich zu überdenken und, wo notwendig, der aktuellen Bedrohungslage anzupassen ist.

8 Domain Name System und Routing

Domain Name System

Zur Nutzung des Internets stehen dem Anwender Dienste wie E-Mail oder das World Wide Web (WWW) zur Verfügung. Eine grundlegende Basis für die Funktion vieler Internetdienste stellt der für die Namensauflösung zuständige DNS (Domain Name System)-Dienst dar. Im Internet gebräuchliche Hostnamen wie www.bsi.bund.de werden mit Hilfe des Domain Name Systems in IP-Adressen umgewandelt (im Beispiel 77.87.228.49). Auf diese Weise muss der Nutzer die nur schwer zu merkenden IP-Adressen in der Regel nicht direkt verwenden. Die Integration der Hostnamen beziehungsweise des DNS in nahezu alle gebräuchlichen Internetdienste macht das Domain Name System zu einem der wichtigsten Dienste im Internet.

Domain Name System

Das bei der Kommunikation zwischen den einzelnen DNS-Servern zum Datenaustausch verwendete Protokoll weist konzeptionelle Schwachstellen auf. Angriffe auf das Protokoll können dazu führen, dass DNS-Informationen im Internet durch Dritte manipuliert werden. 2010 bestand dieses Problem unverändert fort, und es gab einige Beispiele für die Verfälschung von Daten. So wurde Traffic zu populären Webseiten wie YouTube, Twitter und Facebook zum Teil auf Server in China umgeleitet. Zur Verbesserung des zugrunde liegenden Protokolls wurde seitens der Internet Engineering Task Force (IETF) die Protokollerweiterung DNSSEC (Domain Name System Security Extensions) spezifiziert, mit deren Hilfe sowohl die Signierung als auch die Validierung der Domain-Daten möglich ist.

Top-Level-Domains

Top-Level-Domain	Anzahl Second-Level-Domains	DNSSEC Unterstützung
.com	95.006.677	vorhanden
.de	14.369.495	vorhanden
.net	14.003.416	vorhanden
.org	9.639.660	vorhanden
.uk	9.373.754	vorhanden
.info	8.200.168	vorhanden
.nl	4.442.413	vorhanden
.cn	3.379.441 (Stand 28.02.2011)	nicht vorhanden
.eu	3.341.775	vorhanden
.biz	2.254.683	vorhanden

Quelle: BSI

Abb. 11: Die zehn größten Top-Level-Domains [7]

Die Betreiber reagieren

Damit die mit DNSSEC eingeführten Verbesserungen wirksam werden, ist es allerdings erforderlich, dass diese Erweiterung innerhalb der gesamten DNS-Infrastruktur aktiv umgesetzt wird. Während sowohl die Domainverwalter – die so genannten Domain-Registrare – als auch die Internetzugangsanbieter (Internet Service Provider ISP) bei der Umsetzung von DNSSEC noch zurückhaltend sind, gab es im letzten Jahr bei den Betreibern der zugrunde liegenden Basisinfrastruktur einige Veränderungen. So wird DNSSEC beispielsweise seit dem 15. Juli 2010 durch die Wurzel des Domain Name Systems, der so genannten Root-Zone, unterstützt. Auch die Anerkennung durch Top-Level-Domains ist in den letzten zwei Jahren stark gewachsen. So akzeptieren im Mai 2011 bereits 72 von 310 Top-Level-Domains die DNSSEC-Erweiterungen, Anfang 2009 boten lediglich fünf Top-Level-Domains diese Unterstützung. Erfreulicherweise haben damit bis auf China (.cn) die zehn größten Top-Level-Domains bereits DNSSEC umgesetzt. Darunter befindet sich auch die deutsche Top-Level-Domain .de, deren Betreiber DENIC eG DNSSEC zum 31. Mai 2011 eingeführt hat.

Fazit:

Die Umsetzung von DNSSEC erhöht nachhaltig die Sicherheit im Internet und bietet Schutz gegen zahlreiche Gefährdungen. Es ist daher wünschenswert, dass bald auch Domain-Registrare und ISPs die für DNSSEC erforderlichen Umstellungen vornehmen und so die derzeit bestehende Schwachstelle im Domain Name System geschlossen wird. Nach Einschätzung des BSI sprechen aus technischer Sicht keine Argumente gegen die Implementierung von DNSSEC. So wird etwa die Domain .bund.de seit April 2010 erfolgreich mit DNSSEC betrieben.

Routing

Angriff auf die Verfügbarkeit der Internet-Infrastruktur

Eine weitere Möglichkeit, die Strukturen des Internets für Angriffe zu nutzen, besteht beim Routing zwischen den angeschlossenen Systemen. Denn die Struktur des Internets ergibt sich dadurch, dass Netze unterschiedlicher Provider zusammengeschaltet werden. Die Informationen, über welche Netze und Leitungen die angeschlossenen Systeme erreicht werden können (Routing), werden über das Border-Gateway-Protokoll (BGP) ausgetauscht. Dabei existieren Kontrollmechanismen, die eine zuverlässige Überprüfung der untereinander ausgetauschten Informationen ermöglichen würden, nur sehr eingeschränkt. Dies führt dazu, dass jemand mit Zugriff auf die BGP-Infrastruktur die übermittelten Routing-Informationen manipulieren kann. In der Folge einer solchen Manipulation kann beispielsweise ein Netz nicht mehr erreichbar sein.

In der Vergangenheit hat es im Internetrouting bereits häufiger Störungen gegeben. Der letzte große Vorfall, bei dem insgesamt 37.000 Netze betroffen waren, ereignete sich am 8. April 2010. Dabei wurden die an diese Netze gerichteten Datenpakete partiell in Richtung China umgeleitet.

Fazit:

Routing-Manipulationen stellen zur Zeit eine ernstzunehmende Bedrohung dar. In der Fachwelt wird derzeit ein Verfahren entwickelt, mit dem Netzbetreiber zukünftig unberechtigte Änderungen an der BGP-Infrastruktur leichter erkennen können. Diese Verfahren stehen jedoch aktuell noch nicht zur Verfügung. Netzbetreiber sollten daher die Erreichbarkeit ihrer Netze überwachen und geeignete Verschlüsselungsverfahren bei der Übertragung von sensiblen Informationen über das Internet einsetzen.

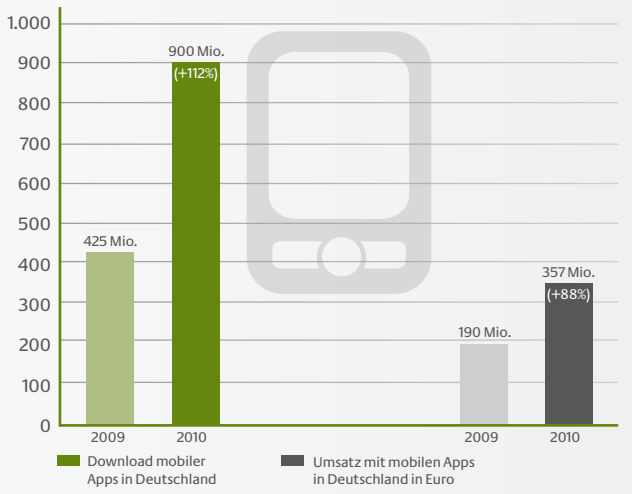
9 Mobilkommunikation

Da immer häufiger wichtige Geschäftsdaten auch von unterwegs genutzt, verarbeitet und über Mobilfunkschnittstellen übertragen werden, rechnet das BSI auch künftig mit einer Zunahme von Angriffen gegen mobile Endgeräte. Rund zehn Millionen Menschen in der Bundesrepublik nutzen regelmäßig die Internetfunktionen ihres Handys.[5] Bis Ende 2010 wurden bereits 900 Millionen Applikationen (Apps) auf Mobiltelefone heruntergeladen.[6]

Smartphone-Nutzer sind sich der Gefahren bei der Anwendung mobiler Betriebssysteme nur teilweise bewusst. So wissen rund 60 Prozent der vom BSI befragten Smartphone-Nutzer, dass ihre mobilen Endgeräte die gleichen Sicherheitsanforderungen haben wie ein PC, was Sicherheitsupdates und Schutzsoftware betrifft. 47 Prozent der Nutzer haben aber noch nie Sicherheitsupdates auf ihr Mobiltelefon eingespielt, nur 20 Prozent tun dies mindestens wöchentlich, elf Prozent mindestens monatlich.[7]

Gefährdungen an der Funkschnittstelle

Mobile Applikationen



Quelle: Bitkom

Abb. 12: Entwicklung von Download und Umsatz mobiler Applikationen für Smartphones in Deutschland [6]

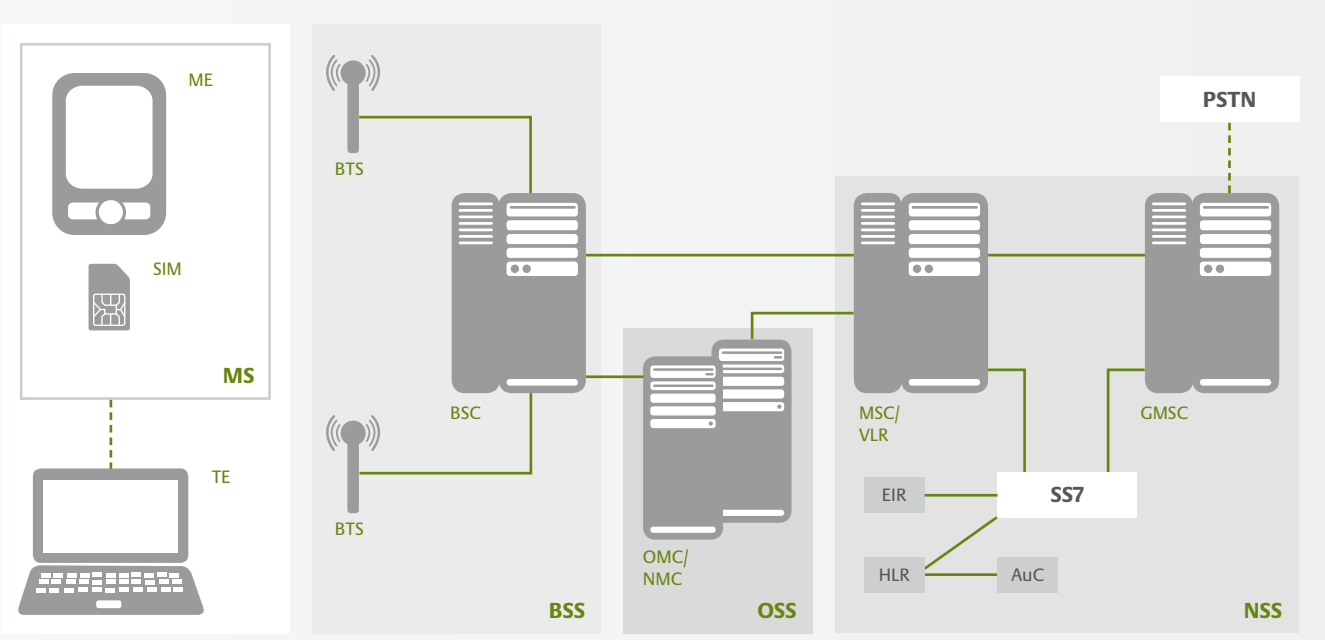
GSM-Standard

Ursprünglich benannt nach der Groupe Spéciale Mobile, steht GSM heute für Global System for Mobile Communications und bezeichnet den weltweit meistverbreiteten Standard für digitale Mobilfunknetze. Ein GSM-Netz besteht aus vier Teilsystemen, der Mobile Station (MS), dem Base Station Subsystem (BSS), dem Operations and Support System (OSS) und dem Network Subsystem (NSS). Die Mobile Station (MS) integriert sich in das GSM-Netz, indem es über die Luftschnittstelle, das heißt über die Funkschnittstelle zwischen dem GSM-Endgerät (ME) und einer Basisstation (BTS) des GSM-Mobilfunknetzes (Um-Schnittstelle), eine Kommunikationsverbindung mit einem Base Station Subsystem (BSS) aufbaut.

Eine besonders signifikante Bedrohung bei der Verwendung von Smartphones ist die Unsicherheit der GSM-Schnittstelle. Der Nutzer muss im Falle ungenügender Absicherung damit rechnen, dass sowohl seine Verbindungs- (zum Beispiel Telefonnummern und Anrufzeitpunkte) als auch seine Nutzdaten (zum Beispiel Gesprächsdaten, E-Mails und SMS) abgehört werden oder dass ein Angreifer Kenntnis über seinen Aufenthaltsort und sein Bewegungsprofil erlangt.

Denn alle Nutzdaten auf der GSM-Luftschnittstelle werden gemäß GSM-Standard verschlüsselt. Doch ist diese Chiffre nicht mehr auf dem Stand der Zeit, und Werkzeuge zum Abhören der GSM-Kommunikation sind längst verfügbar.

So können die GSM-Schlüssel von einem Datendieb ermittelt werden, wenn es gelingt, die Datenkommunikation an der GSM-Luftschnittstelle mitzuschneiden. Die Kenntnis des Schlüssels erlaubt dann das Dekodieren von GSM-Gesprächsdaten und ggf. sogar von SMS. Nicht betroffen davon sind Datenverbindungen über UMTS (Universal Mobile Telecommunications System), GPRS (General Packet Radio Service) und EDGE (Enhanced Data Rates für GSM Evolution) sowie Telefonate über UMTS.



Quelle: BSI

Abb. 13: Vereinfachte Darstellung eines GSM-Mobilfunknetzes [7]

Weitere Sicherheitsgefährdungen bei der Nutzung mobiler Endgeräte sind:

- Abhören im „Backend“: Der Angreifer fasst die Gesprächsdaten per Kabel ab, das die Telefonate unverschlüsselt überträgt.
- das Laden und Installieren von Schadsoftware aus dem Internet sowie die Manipulierbarkeit mobiler Endgeräte durch Trojaner-Software. Schadsoftware kann ein Smartphone unbrauchbar machen und überdies mit dem Telefon vernetzte IT-Systeme infizieren. Mit einem Trojanischen Pferd infizierte Mobiltelefone lassen sich sogar als Abhörwanzen nutzen, die über die Mobilfunkschnittstelle ferngesteuert werden. Schließlich können auch Nutzerdaten ausgespäht und an den Datendieb geschickt werden.
- Treten zusätzliche beziehungsweise fehlende Verbindungen auf einem Einzelverbindungsnachweis eines Mobilfunknutzers auf, so kann dies ebenfalls ein Hinweis auf eine Attacke sein, zum Beispiel per Trojanischem Pferd.
- Man-in-the-Middle-Angriff: Hierbei ahmt der Angreifer eine GSM-Basisstation nach. Dies ist relativ leicht möglich, da hierfür keine Authentisierung gegenüber dem Endgerät erforderlich ist. Dann nimmt er eine Position zwischen Endgerät und Mobilfunknetz ein und deaktiviert die GSM-Verschlüsselung.

Fazit:

Da GSM-Telefonate grundsätzlich unsicher sind, sollten sensible Informationen nicht bedenkenlos über die entsprechenden Endgeräte ausgetauscht werden. Alternativen, die zumindest eine sicherere Verschlüsselung auf der Luftschnittstelle ermöglichen, stehen mit GPRS, UMTS und künftig mit LTE (Long Term Evolution) zur Verfügung. Für den besseren Schutz bei der Anwendung von mobilen Endgeräten empfiehlt das BSI, keine Software aus unbekannten Quellen zu installieren und nur tatsächlich benötigte Applikationen zu installieren beziehungsweise zu aktivieren. Außerdem sollten Mobiltelefone zur Verbesserung der IT-Sicherheit „minimal offen“ konfiguriert werden. Beispielsweise sollten lokale Funkschnittstellen wie WLAN (Wireless Local Area Network) oder Bluetooth nur bei Bedarf aktiviert und dann mit bestmöglichen Sicherheitseinstellungen und nur unter Freigabe der benötigten Funktionen betrieben werden. Für den Austausch von Informationen mit Schutzbedarf sollten immer kryptographische Lösungen eingesetzt werden, die mit einem Hardware-Sicherheitsanker (Krypto-Smartcard beziehungsweise Krypto-Modul) ausgestattet sind.

10/11 Zukunftsthemen

10 Cloud Computing

Cloud Computing

Unter Cloud Computing versteht man ein Modell, das es erlaubt, IT-Dienstleistungen (Software-as-a-Service, Platform-as-a-Service, Infrastructure-as-a-Service) jederzeit, netzbasiert, schnell und dem tatsächlichen Bedarf angepasst sowie nach tatsächlicher Nutzung abrechenbar zu beziehen. Hierbei können die Services entweder aus einer Public, Private oder Hybrid Cloud bezogen werden. Bei einer Public Cloud werden die IT-Dienstleistungen von einem Cloud-Anbieter bereitgestellt und können von jedem über das Internet genutzt werden. Alternativ dazu können die Anwender eine entsprechende Infrastruktur selbst aufbauen und die IT-Dienstleistungen aus den eigenen Rechenzentren beziehen (Private Cloud). In einer Private Cloud unterstehen alle Dienste und die Infrastruktur der Institution, die die angebotenen Services nutzt. Die Cloud kann aber durchaus von Dritten betrieben werden. Auf die Dienste kann über das Intranet oder über VPN (Virtual Private Network) zugegriffen werden. Eine Hybrid Cloud ist eine Mischform, bestehend aus einer Public Cloud und einer Private Cloud.

Das Thema Cloud Computing ist in der Informationstechnik allgegenwärtig und hat in den letzten Jahren weltweit immens an Bedeutung gewonnen. Auch in Deutschland rechnen die Marktforscher mit enormen Zuwächsen bei Ausgaben für Cloud Services in den kommenden Jahren. Schätzungsweise werden die Umsätze für Cloud-Dienstleistungen in Deutschland von 1,14 Milliarden Euro 2010 auf mögliche 8,2 Milliarden Euro im Jahr 2015 steigen. Dies entspricht einer jährlichen Steigerung des Umsatzwachstums von durchschnittlich 48 Prozent.[8]

Die Gründe für das zunehmende Interesse am Thema Cloud Computing und die steigende Nutzung von Cloud-Diensten sind vielfältig. Cloud Computing verspricht enorme Flexibilität bei der Buchung und Nutzung sowie Stilllegung von Rechenzentren-Kapazitäten, je nach aktuellem Bedarf. Erwartet wird auch ein hohes Einsparpotenzial im Bereich der ansonsten lokal vorzuhaltenden, zu wartenden und in kurzen Zyklen zu erneuernden IT-Systeme. Ein weiterer Vorteil ist die ubiquitäre Verfügbarkeit von Geschäftsanwendungen, unabhängig vom geografischen Standort des Anwenders.

Chancen und Risiken abwägen

Diesen potenziellen Vorteilen steht eine Reihe von Risiken gegenüber, die mit einer Auslagerung der Daten beziehungsweise Anwendungen in eine Public Cloud verbunden sind, so etwa:

- Daten beziehungsweise Anwendungen werden außer Haus verlagert und sind somit dem direkten Zugriff durch die eigene IT entzogen.
- Geltende Richtlinien und Vorgaben wie zum Beispiel Datenschutzanforderungen könnten verletzt werden, wenn beispielsweise sensitive Daten in eine Public Cloud ausgelagert werden.
- Viele unbekannte Nutzer teilen sich eine gemeinsame Infrastruktur. Damit steigt das Risiko, dass die Grundwerte der Informationssicherheit verletzt werden.
- Daten und Anwendungen werden über das Internet genutzt, so dass ein Ausfall der Internetverbindung den Zugriff unmöglich macht.
- Sind die Schnittstellen, die ein Cloud-Anbieter zur Verfügung stellt, unsicher programmiert, dann können Schwachstellen ausgenutzt werden, um unerlaubt auf Daten zuzugreifen.
- Durch die sehr hohe Komplexität von Cloud Computing-Plattformen, der Fülle an Konfigurationseinstellungen und der sich gegenseitig beeinflussenden Parameter, können zahlreiche Sicherheitsprobleme entstehen wie zum Beispiel Datenverlust, unerlaubter Zugriff auf Informationen, Beeinträchtigung der Verfügbarkeit oder sogar Ausfall von Diensten.

Nach Einschätzungen des BSI ist zu erwarten, dass sich das Konzept des Cloud Computing aufgrund der technischen und wirtschaftlichen Potenziale am Markt durchsetzen wird, wenn die Frage der angemessenen Informationssicherheit geklärt wird. Mit zunehmender Verbreitung in der Fläche wird das Konzept auch aufgrund der Konzentration der Ressourcen in zentralen Rechenzentren für Angreifer attraktiver. Bereits heute werden Cloud Computing-Plattformen zum Aufbau von Botnetzen, zur Ablage von Schadprogrammen, zum Versenden von SPAM oder zur Durchführung von Brute-Force-Angriffen auf Passwörter missbraucht. Darüber hinaus sind einige Fälle bekannt geworden, bei denen Cloud Computing-Plattformen Ziel von DDoS-Angriffen geworden sind.

Fazit:

Ein zunehmendes Gefährdungspotenzial wird prognostiziert. Aus diesem Grund ist es notwendig, international anerkannte Standards zu erarbeiten und zu etablieren, auf deren Grundlage Cloud Computing-Plattformen sicherer genutzt und betrieben sowie überprüft und zertifiziert werden können.

11 Smart Grid / Smart Meter

Smart Grid / Smart Meter

Seit dem 1. Januar 2010 müssen in Neubauten oder bei größeren Hausrenovierungen grundsätzlich Stromzähler eingebaut werden, die – im Gegensatz zu den herkömmlichen Messgeräten – dem Nutzer den tatsächlichen Energieverbrauch und die tatsächliche Nutzungszeit widerspiegeln. Überdies sollen die neuen Stromzähler aus der Ferne ablesbar und steuerbar sein. Um die Verbraucher zu einem klimafreundlichen Verhalten anzuregen, sind die Energieversorger außerdem seit Ende des Jahres 2010 verpflichtet, flexiblere Verbrauchstarife anzubieten, die sich an der Netzauslastung oder der Tageszeit orientieren. Smart Grid steht als Schlagwort für die Entwicklung hin zu ganzheitlichen, intelligenten Versorgungssystemen. Das betrifft vor allem die Stromnetze, aber auch die Energie- und Wasserversorgung allgemein. In der Elektrizitätsversorgung ist diese Entwicklung zwingend notwendig, um den wachsenden Anteil von dezentral erzeugter und ins Stromnetz eingespeister Elektrizität zu bewältigen. Daneben muss mittelfristig auch der zeitliche Verlauf des Stromverbrauchs optimiert werden. Dies ist mit den vorhandenen hierarchischen, elektrophysikalischen Verbundnetzen nicht zu bewältigen. Stattdessen sind neue, vernetzte Steuerungstechnologien gefragt.

Das weltweite Marktvolumen für Smart-Grid-Technologien könnte nach Schätzungen des US-amerikanischen Unternehmens Cisco Systems ein 100 Mal größeres Potenzial als das Internet erreichen. Die zunehmende Komplexität der Elektrizitätsnetze erfordert zudem neue Formen der Absicherung des Gesamtsystems gegen Ausfälle. Entsprechende Mechanismen sollen vernetzte informationstechnische Systeme nutzen, die allerdings teilweise noch entwickelt und implementiert werden müssen.

Da Energie- und Wasserversorgungssysteme unverzichtbar sind, muss bei dieser Arbeit die heute gegebene, sehr hohe Versorgungssicherheit erhalten bleiben. Sie darf keinesfalls durch Ausfälle, Störungen oder Angriffe auf die nun zu implementierenden informationstechnischen Infrastrukturen gefährdet werden – und muss dabei auch in Krisenlagen die notwendige Robustheit aufweisen. Zudem ergeben sich künftig spezielle Risiken daraus, dass bestimmte Teilinfrastrukturen zwischen unterschiedlichen Betreibern komplex vernetzt werden. Dies gilt vor allem dann, wenn diese Vernetzung über Informationsinfrastrukturen erfolgt, über die teils sehr unterschiedliche Anwendungen mit einer großen Anzahl an Kommunikationsteilnehmern abgewickelt werden, oder falls der Informationsaustausch über das offene Internet erfolgen soll.

Smart Meter – intelligente Zähler

Flexibel steuerbare Netze zu entwerfen und aufzubauen, ist also das Gebot der Stunde. Der Weg zu ganzheitlichen, intelligenten Versorgungssystemen ist dabei noch weit. Die fachlichen Grundlagen dazu müssen in den betroffenen Sektoren noch deutlich weiterentwickelt werden. In den Versorgungsinfrastrukturen werden aber bereits jetzt erste Schritte unternommen. Hier befinden sich diverse Technologien bereits in der Spezifikation, der Realisierungsphase oder gar schon in der Implementierung. Das BSI begleitet die Entwicklung der fachlichen Grundlagen für intelligente Stromversorgungssysteme und sorgt so dafür, dass die wichtigen Aspekte der IT-Sicherheit dabei berücksichtigt werden. Ein wichtiger Grundbaustein in der Fortentwicklung der Versorgungsinfrastrukturen stellt die Einführung von so genannten „Smart Metern“ (Intelligente Zähler) dar. Aufgrund der Verarbeitung und Zusammenführung personenbezogener Verbrauchsdaten im Smart Meter sowie möglicher negativer Rückwirkungen auf die Energieversorgung, ergeben sich Anforderungen sowohl an den Datenschutz als auch an die IT-Sicherheit der intelligenten Messgeräte.

Fazit:

Bekannt gewordene Hackerangriffe auf Smart Meter in den USA und Gefährdungen wie Stuxnet haben zuletzt gezeigt, dass in Deutschland ein akuter Handlungsbedarf für sichere Smart Metering-Lösungen besteht. Das BSI wird daher in Zusammenarbeit mit Wirtschaftsverbänden und relevanten Behörden, wie zum Beispiel der Bundesnetzagentur und der Physikalisch-Technischen Bundesanstalt (PTB) die Sicherheitsanforderungen für Smart Meter in einem eigenen Schutzprofil bündeln, um verbindliche Sicherheitsanforderungen von Datenschutz und Datensicherheit für alle Marktteilnehmer zu gewährleisten. Es ist geplant, bis zum September 2011 eine vom BSI zertifizierte Version des Schutzprofils vorzulegen. Des Weiteren wird das BSI eine Technische Richtlinie erstellen, in der Anforderungen an die Interoperabilität von Smart Metern beschrieben werden.

Fazit

Aufgrund der Durchdringung von IT in allen Lebensbereichen und der fast durchgängigen Vernetzung sind wir auf ein fehlerfreies Funktionieren der Informationstechnik angewiesen. Nach Einschätzung des BSI und anderer Sicherheitsbehörden stellen die parallel zu dieser Entwicklung entstehenden neuen Gefährdungen – wie Cyberangriffe, Angriffe auf mobile Endgeräte und Attacken, die auch außerhalb der klassischen IT greifen – eine gemeinsame Herausforderung für Politik, Wirtschaft und Gesellschaft dar.

Angebote, die Bundesverwaltung, Wirtschaft und Bürgern im Bedarfsfall reaktiv Hilfestellung bieten, sind notwendig und erfüllen eine wichtige Funktion. Um der Gefährdungslage wirksam zu begegnen, gilt es jedoch, noch stärker auf Prävention zu setzen. Um ein grundsätzliches IT-Sicherheitsniveau zu gewährleisten und Gefahren möglichst vorab zu antizipieren, ist es zunehmend bedeutsam, Sicherheitsanforderungen an Produkte und Dienstleistungen zu formulieren und auch öffentlich transparent zu machen. Das BSI verfolgt diesen Ansatz mit der Formulierung von Mindeststandards, wie zum Beispiel im Cloud Computing. Hierdurch wird die technische Basis für Vertrauen in sichere Informationstechnik und für die Ausschöpfung ihrer Potenziale gelegt. Zudem gelangt die Verantwortung der Hersteller- und Dienstleistungsanbieter noch stärker in den öffentlichen Fokus.

IT-Sicherheit zu stärken ist ein Ziel, das nur durch effektive Zusammenarbeit erreicht werden kann. Der Erfolg ist abhängig vom Zusammenwirken der Hersteller, Provider, der Sicherheitsexperten und -verantwortlichen und nicht zuletzt der Anwender, deren Bewusstsein für die Umsetzung von Sicherheitsmaßnahmen in der Fläche eine wichtige Rolle spielt.

BSI – IT-Sicherheit im Fokus

Mit dem Koalitionsvertrag und dem BSI-Gesetz vom August 2009 reagiert die Bundesregierung und weist dem BSI eine stärkere Rolle als IT-Sicherheitsgestalter und -dienstleister zu. Der Koalitionsvertrag unterstreicht auch die Aufgabe des BSI für mehr Selbstschutz zu werben und die Nutzung sicherer IT-Produkte anzuregen.

Aufklärung und Sensibilisierung

Im Bereich Aufklärung und Sensibilisierung der Bürger ist das BSI bereits langjährig tätig. So gibt es das Informationsportal BSI für Bürger: Nach wie vor stellt das Online-Angebot www.bsi-fuer-buerger.de das wichtigste Informationsangebot für Privatnutzer dar. Seit Februar 2011 steht den Bürgern ein überarbeitetes und verbessertes Angebot zur Verfügung, welches ihnen umfassende und leicht verständliche Informationen zum Thema IT-Sicherheit gibt und ihnen den Schutz ihres Computers erleichtert.

Gemeinschaftliches Handeln

Aufklärung und Sensibilisierung im Bereich IT-Sicherheit hat viele unterschiedliche Facetten. Dem Austausch und der Zusammenarbeit mit Kooperationspartnern und Multiplikatoren kommt daher eine besondere Bedeutung zu. So ist das BSI im Beirat des Vereins Deutschland sicher im Netz e.V. vertreten und unterstützt das Anti-Botnet-Beratungszentrum des eco-Verbands der deutschen Internetwirtschaft e.V., welches im Herbst 2010 in Betrieb genommen wurde. Auf internationaler Ebene beteiligt sich das BSI in der Awareness Raising Community der ENISA (European Network and Information Security Agency), zudem nimmt es mit Aktionen am jährlich stattfindenden Aktionstag „Safer Internet Day“ der Europäischen Union teil.

IT-Sicherheitsdienstleister des Bundes

Das BSI als zentraler IT-Sicherheitsdienstleister des Bundes verbessert das IT-Sicherheitsniveau in der Bundesverwaltung. Insbesondere bei IT-Krisen nationaler Bedeutung muss durch aufbereitete Informationen und kompetente Analysen die Entscheidungs- und Handlungsfähigkeit der Bundesregierung sichergestellt werden. Dazu wurde das IT-Krisenreaktionszentrum des Bundes im BSI aufgebaut, mit der Novellierung des BSI-Gesetzes das BSI unter anderem als zentrale Meldestelle für IT-Sicherheitsvorfälle etabliert und ein IT-Krisenmanagement für die Bundesverwaltung geschaffen. So entstand ein Frühwarnsystem der Bundesverwaltung, welches die Erstellung von Lagebildern ermöglicht, Krisenreaktionsprozesse definiert und auf Grundlage des Krisenmanagements beübt wird.

Zusammenarbeit bei IT-Krisen

Über einen gezielten und hochwertigen Angriff wie Stuxnet ist lange theoretisch diskutiert worden, nun ist erstmalig der exemplarische Nachweis da: Schutzmechanismen können mit entsprechendem finanziellen Aufwand und technischer Vorbereitung gezielt umgangen und unterlaufen werden. Auf diese neue Qualität der Angriffe muss reagiert werden, denn Angriffsmechanismen wie bei Stuxnet orientieren sich nicht an der klassischen Aufgabenteilung deutscher Behörden. Stuxnet zeigt, dass eine noch engere Abstimmung zwischen den Behörden sowie eine intensivere Zusammenarbeit mit der Wirtschaft benötigt wird. Deswegen hat die Bundesregierung 2011 die Cyber-Sicherheitsstrategie verabschiedet, die den Aufbau eines Cyber-Abwehrzentrums unter Federführung des BSI und direkter Beteiligung des Bundesamtes für Verfassungsschutz und des Bundesamtes für Bevölkerungsschutz und Katastrophenhilfe sowie der Beteiligung weiterer Behörden vorsieht. Der Ausbau der Zusammenarbeit mit der Wirtschaft ist ebenfalls vorgesehen.

Vertrauen in die Sicherheit der Technik

Die Möglichkeiten und Potenziale der IT und des Internets werden nur genutzt, wenn Vertrauen in die Sicherheit der Technik beziehungsweise Technologie besteht. Qualitätssiegel von berufenen Stellen und etablierte IT-Sicherheitsstandards sind das Fundament für dieses Vertrauen. Mit Blick auf IT-Sicherheitsstandards bringt sich das BSI beispielsweise in zukunftsweisende Projekte wie Smart Meter, intelligente Zähler für die Energieversorgung, oder Cloud Computing ein. Im Bereich Smart Meter erstellt das BSI gemeinsam mit Wirtschaft, Daten- und Verbraucherschützern ein gemeinsames Schutzprofil. Ziel ist es, ein angemessenes Sicherheitsniveau zu erreichen, das sowohl Funktionalität als auch Datenschutz und IT-Sicherheit in adäquater Weise berücksichtigt. Auch beim Cloud Computing werden gemeinsam mit Herstellern Mindestsicherheitsanforderungen erstellt. In Ergänzung stellt die Zertifizierung des BSI sicher, dass vorgeschriebene Sicherheitsstandards in Produkten auch gewährleistet beziehungsweise durchgesetzt werden.

Zwei wichtige Projekte, an deren technischer Umsetzung das BSI maßgeblich beteiligt war und die im Hinblick auf sichere Kommunikation und Interaktion im Internet einen Sicherheitsgewinn bedeuten, sind der neue Personalausweis und De-Mail. Mit De-Mail wird das verbindliche und vertrauliche Versenden von Dokumenten und Nachrichten über das Internet möglich. De-Mail erhöht die Sicherheit der elektronischen im Vergleich zur herkömmlichen Kommunikation. Die wesentlichen Sicherheitsziele Vertraulichkeit, Integrität und Authentizität bei der De-Mail-Kommunikation werden durch definierte Sicherungsmaßnahmen gewährleistet. Mit De-Mail können die Identität der Kommunikationspartner sowie die Zustellung der De-Mails nachgewiesen werden. Die Inhalte einer De-Mail können auf ihrem Weg durch das Internet nicht mitgelesen oder gar verändert werden.

Mit dem neuen Personalausweis steht dem Bürger seit November 2010 nicht nur ein Sichtausweis im neuen Scheckkartenformat zur Verfügung. Das Ausweisdokument bietet zusätzlich verschiedene elektronische Funktionen, die auch im Internet für deutlich mehr Sicherheit sorgen. Dazu zählt zum einen der elektronische Identitätsnachweis, die so genannte eID, mit der sich der Bürger zweifelsfrei online ausweisen kann. Ein in den Ausweis integrierter Radio Frequency-Chip (RF-Chip) enthält dazu alle Informationen, die auch visuell von dem Dokument ablesbar sind. Mit der QES-Funktion, der qualifizierten elektronischen Signatur, kann der Nutzer darüber hinaus Dokumente und Willenserklärungen rechtssicher online unterschreiben.

Kritische Infrastrukturen (KRITIS)

Ein besonderes Augenmerk in der Zusammenarbeit mit der Wirtschaft liegt auf dem Schutz Kritischer Infrastrukturen, einer Gemeinschaftsaufgabe der Betreiber und des Staates. Das BSI und Betreiber der Kritischen Infrastrukturen in Deutschland arbeiten seit 2007 auf Basis des Umsetzungsplans KRITIS (UP KRITIS) eng zusammen, um neue Bedrohungen und Strategien zu diskutieren und Maßnahmen zu realisieren. Um auf einen möglichen Vorfall vorbereitet zu sein, finden regelmäßig Übungen statt. Eines der wesentlichen Übungsformate ist die so genannte LÜKEX (Länder Übergreifende Krisenmanagement-Übung/ Exercise). Im Jahr 2011 werden die KRITIS-Unternehmen hieran intensiv beteiligt sein, da in diesem Jahr der Ausfall wesentlicher IT-Systeme und das Krisenmanagement in dieser Ausnahmesituation geübt werden sollen.

Quellenverzeichnis

[1] Secunia Yearly Report 2010

[2] http://gs.statcounter.com/press/firefox-overtakes-internet-explorer-in-europe-in-browser-wars

[3] Trendmicro 16.09.2009 http://blog.trendmicro.com/the-internet-infestation-how-bad-is-it-really/

[4] Damballa 14. Februar 2011 http://www.damballa.com/knowledge/Feb2011report.php

[5] BITKOM Presseinformation vom 15. August 2010

[6] BITKOM Presseinformation vom 14. Februar 2011

[7] BSI-Erhebungen

[8] BITKOM-Presseinformation vom 6. Oktober 2010

[9] Arbor Worldwide Infrastructure Security Report 2010

Abbildungsverzeichnis

Herausgeber
Bundesamt für Sicherheit in der Informationstechnik – BSI
53175 Bonn

Texte und Redaktion
Bundesamt für Sicherheit in der Informationstechnik
DauthKaun Public Relations

Layout und Gestaltung
DauthKaun Werbeagentur

Druck
Druckpartner Moser, Rheinbach

Stand
Mai 2011

Artikelnummer
BSI-LB11502

Bezugsstelle
Bundesamt für Sicherheit in der Informationstechnik – BSI
Godesberger Allee 185 - 189, 53175 Bonn

Referat 321 – Information, Kommunikation, Öffentlichkeitsarbeit
Tel.: +49 228 99 9582-0, E-Mail: publikationen@bsi.bund.de
Internet: www.bsi.bund.de