



Bundesamt
für Sicherheit in der
Informationstechnik

The background of the cover is a vibrant blue with a complex, abstract design. It features overlapping, semi-transparent geometric shapes, including large triangles and curved bands. A pattern of fine, parallel lines creates a sense of depth and movement. In the lower-left quadrant, several stylized arrows, composed of a grid of small dots, point towards the right. The overall effect is one of modernity and technological sophistication.

Die Lage der IT-Sicherheit in Deutschland 2014

Inhaltsverzeichnis

Vorwort	4
1 Informationstechnik: vernetzt, komplex, allgegenwärtig	6
2 Gefährdungslage	10
2.1 Ursachen	11
2.1.1 Angriffsplattform Internet	11
2.1.2 „Digitale Sorglosigkeit“	12
2.1.3 Schwachstellen	12
2.1.4 Einsatz veralteter Software und ungepatchter Systeme	13
2.1.5 Mobile Endgeräte	14
2.1.6 Unzureichende Absicherung industrieller Steuerungssysteme	14
2.2 Angriffsmittel und -methoden	15
2.2.1 Spam	15
2.2.2 Schadprogramme	16
2.2.3 Drive-by-Exploits und Exploit-Kits	17
2.2.4 Botnetze	18
2.2.5 Social Engineering	19
2.2.6 Identitätsdiebstahl	20
2.2.7 Denial of Service	20
2.2.8 Advanced Persistent Threats (APT)	21
2.2.9 Nachrichtendienstliche Cyber-Angriffe	22
2.3 Angreifer-Typologie	23
2.3.1 Cyber-Kriminelle	23
2.3.2 Nachrichtendienste	24
2.3.3 Hacktivismus und Cyber-Aktivisten	24
2.3.4 Innentäter	25
2.4 Zusammenfassung	25

3	Vorfälle	27
3.1	Vorfälle in der Bundesverwaltung	28
3.2	Vorfälle bei Privatanwendern	29
3.2.1	Millionenfacher Identitätsdiebstahl in Deutschland	29
3.2.2	Schwachstellen in Routern für Heimnetzwerke	29
3.2.3	Online-Banking-Trojaner: von Feodo zu Geodo	30
3.2.4	iBanking: Schadsoftware für Smartphones	30
3.3	Vorfälle in der Wirtschaft	31
3.3.1	APT-Angriff auf Industrieanlagen in Deutschland	31
3.3.2	Heartbleed – Kritische Schwachstelle in weit verbreiteter Softwarebibliothek	31
3.3.3	Dragonfly – gezielte Angriffe auf Produktionsnetze	32
3.3.4	Operation Windigo – Linux-Schadprogramm Ebury sammelt SSH-Zugangsdaten	32
3.3.5	Großbritannien: Bankrott infolge von Cyber-Erpressung und Sabotage	33
3.3.6	ShellShock – Schwachstelle im Kommandozeileninterpreter Bash	33
3.4	Vorfälle im Bereich Kritischer Infrastrukturen (KRITIS)	34
3.4.1	Social Engineering bei Großkonzernen	34
3.4.2	Österreich: Fehlfunktion in der Steuerung von Energienetzen	34
3.4.3	USA: IT-Manipulation im Hochfrequenzhandel eines US-Hedgefonds	35
4	Lösungsansätze	36
4.1	Kompetenz und Vertrauenswürdigkeit im Bereich IT-Sicherheit fördern	37
4.2	Engagement in Standardisierung und Zertifizierung	37
4.3	IT-Sicherheit in der Gesellschaft und breitflächige Anwendung sicherer Technologien fördern	38
4.4	Schutz Kritischer Infrastrukturen gewährleisten	39
5	Glossar und Abkürzungsverzeichnis	40
6	Abbildungs- und Tabellenverzeichnis und Fußnoten	43

Vorwort

Der Lagebericht zur IT-Sicherheit 2014 informiert über die Qualität und Quantität der Gefährdungen sowie über die sich daraus ergebenden Risiken für die Informationstechnik (IT) in Deutschland. In den Lagebericht sind umfangreiche Informationen sowohl über Gefährdungen, Schwachstellen und Verwundbarkeiten in der IT als auch über akute IT-Angriffe eingeflossen, die beim Bundesamt für Sicherheit in der Informationstechnik (BSI) täglich gesammelt und ausgewertet werden.

Die aktuelle Gefährdungslage für die IT bleibt hinsichtlich des zu verzeichnenden Angriffspotenzials kritisch. Nicht nur die Anzahl schwerer Sicherheitslücken in den meistverbreiteten IT-Systemen rangierten auf sehr hohem Niveau. Auch die Werkzeuge zur Ausnutzung dieser Verwundbarkeiten stehen einer immer größer werdenden Anzahl an Angreifern zur Verfügung, die diese aus der Anonymität des globalen Cyber-Raums für ihre Zwecke einzusetzen bereit sind. Im Fadenkreuz der Angriffe stehen, wenn auch aus unterschiedlichen Motiven heraus, Bürgerinnen und Bürger, staatliche Stellen, Forschungseinrichtungen, Wirtschaftsunternehmen und auch Betreiber Kritischer Infrastrukturen (KRITIS) in Deutschland.

Ohne Frage treibt die durch Informationstechnik beschleunigte Globalisierung den Wettbewerb um Ressourcen, Märkte und politische Einflussbereiche voran. Es wäre naiv anzunehmen, die neu gewonnenen digital vernetzten Technologien würden nicht auch für Auseinandersetzungen in der Wirtschaft, Gesellschaft und Politik ausgenutzt werden. Im Gegenteil ist zu beobachten, dass Wirtschaft und Verwaltung zunehmend von sehr versierten IT-Angriffen betroffen sind, die mit großem Ressourceneinsatz und großer Professionalität ausgeführt werden. Solche Angriffe sind meist nur schwer zu erkennen und abzuwehren. Häufig genug öffnet sich zwischen Angriff und Erkennung ein besorgniserregendes Zeitfenster, in dem der erfolgreiche Angreifer ungehinderten und unbeobachteten Zugriff auf die IT-Systeme erhält.

Die Innovationsgeschwindigkeit der Informationstechnologie ist sehr hoch. Aufgrund der enormen wirtschaftlichen Potenziale treibt sie

damit auch die Veränderung der IT-Landschaften in allen industriellen und gesellschaftlichen Bereichen rasant voran. Cloud Computing, mobile Systeme, Auswertungsmöglichkeiten von Informationen mittels Big Data schaffen einerseits wirtschaftliche Prosperität, aber andererseits auch neue Verwundbarkeiten für IT-Angriffe, die mit den konventionellen Lösungsansätzen der IT-Sicherheit nicht angemessen adressiert werden können. Innovation in der Informationstechnologie muss daher mit der Evolution von IT-Sicherheitsmechanismen Hand in Hand gehen, damit die Verteidiger gegenüber den Angreifern technologisch nicht ins Hintertreffen geraten.

Erfolgreiche IT-Sicherheit erfordert eigenverantwortliches und kompetentes Handeln. Die seit 2013 öffentlich bekannt gewordenen Aktivitäten ausländischer Nachrichtendienste sowie der millionen- und milliardenfache Identitätsdiebstahl haben zu einer Vertrauenskrise im Internet geführt. Wenngleich dadurch die Sensibilität für dieses Thema sprunghaft zunimmt, erleben sich private Nutzer – aber auch professionelle Anwender – immer häufiger in einer subjektiven Situation der Machtlosigkeit gegenüber den anscheinend übermächtigen Bedrohungen. Mitunter werden dann in resignativer Stimmung nicht einmal mehr die durchaus verfügbaren und leistbaren Sicherheitsmaßnahmen ausgeschöpft, mit denen schon ein beachtliches Schutzniveau zu erreichen ist, das bis zu 95 Prozent der gängigen Angriffe abwehrt. Damit bleiben aber Potenziale ungenutzt und verschärfen unnötig die IT-Sicherheitslage.

Hier droht ein Kreislauf sich selbst erfüllender negativer Prophezeiungen zu entstehen, der durchbrochen werden muss. Um das Vertrauen der Nutzer in die Sicherheit der IT wiederherzustellen und auszubauen, kommen der Standardisierung, Zertifizierung und Transparenz wichtige Funktionen zu. Deutschland ist dabei mit einer mittelständisch geprägten IT-Sicherheitswirtschaft technologisch breit und kompetentbaufgestellt. Diese günstigen Voraussetzungenb gilt es, bei der anstehenden Digitalisierung aller Lebens- und Wirtschaftsbereiche zum Vorteil des deutschen Standorts zu nutzen und ein positives Klima für IT-Sicherheitsmaßnahmen zu schaffen.

IT-Sicherheit darf etwas kosten, muss aber im Markt auch belohnt werden.

Mein Wunsch ist, dass Wirtschaft und Staat verstärkt weitergehende Sicherheitstechnologien fordern und ihren Einsatz fördern. Die Bundesregierung treibt dazu die Verbreitung von Basis-Sicherheitsinfrastrukturen beispielsweise mit dem Identitätsnachweis im Internet auf Grundlage des neuen Personalausweises, mit De-Mail oder auch dem Smart-Meter-Profil voran. Wir freuen uns über vorausschauende Unternehmen, die darauf aufbauend smarte und kreative Lösungen verwirklichen und skalierbare IT-Sicherheitsmaßnahmen in den Anwendungen ergänzen, um den IT-Risiken in der digitalisierten Welt angemessen zu begegnen.

Mit dem angestrebten IT-Sicherheitsgesetz wird ein weiterer Baustein zur besseren Absicherung von unverzichtbar werdenden IT-Infrastrukturen gelegt. Die Aufstellung des BSI als zivile, technisch-präventive Behörde hat sich in den vergangenen 20 Jahren bewährt. Daher wird die Rolle des BSI in der Cyber-Sicherheitsarchitektur weiter gestärkt werden. Als vertrauenswürdiger Kompetenzträger wird das BSI bei der Gestaltung der IT-Sicherheitsinfrastrukturen in den Bereichen der Kritischen Infrastrukturen eine beratende und akkreditierende Funktion erhalten. Um Reaktionsgeschwindigkeit zu gewinnen, wird auch der Informationsaustausch über Gefährdungen und Angriffe auf IT-Systeme intensiviert. Denn taugliche und angemessene Sicherheitsmaßnahmen für die Informationstechnik in Deutschland können in Zukunft nur noch in einem kooperativen und partnerschaftlichen Zusammenwirken von Wirtschaft und Staat gewährleistet werden. Das BSI wird daher neben seiner fachlichen Expertise auch als koordinierende Stelle im Verbund mit den weiteren Sicherheitsbehörden des Bundes und der Länder gefordert sein.

Ich bin überzeugt, dass wir mit der robusten Aufstellung des BSI trotz der nicht kleiner werdenden Gefährdungen aus dem Cyber-Raum eine verbesserte Sicherheitslage schaffen werden.



Dr. Thomas de Maizière
Bundesminister des Innern

1 Informationstechnik: vernetzt, komplex, allgegenwärtig

1 Informationstechnik: vernetzt, komplex, allgegenwärtig

Die Digitalisierung prägen drei zentrale Charakteristika, aus denen sich die Herausforderungen für die Informations- und Cyber-Sicherheit ergeben.

- 1** Technologische Durchdringung und Vernetzung: Alle physischen Systeme werden von IT erfasst und schrittweise mit dem Internet verbunden.
- 2** Komplexität: Die Komplexität der IT nimmt durch vertikale und horizontale Integration in die Wertschöpfungsprozesse erheblich zu.
- 3** Allgegenwärtigkeit: Jedes System ist praktisch zu jeder Zeit und von jedem Ort über das Internet erreichbar.

Technologische Durchdringung und Vernetzung

Die heutige Informationstechnik zeichnet sich durch ihre leistungsfähige und Nutzen schaffende Fähigkeit zur Integration in praktisch alle technischen Systeme aus und treibt damit die Digitalisierung unserer Welt voran. Insbesondere durch die funktionell und preislich attraktiven Angebote auch für Privatanwender entwickelt sich ein Markt. So versprechen beispielsweise mobile Lösungen und Applikationen in Verbindung mit intuitiv nutzbaren Endgeräten reizvolle Weiterentwicklungen auch im professionellen Umfeld. Die schnelle Adaption solcher Lösungen in Wirtschaft und Industrie lässt die Grenzen zwischen privat und beruflich genutzter IT verschwinden. Dies führt mittelbar auch dazu, dass die traditionell stark getrennten IT-Netze von Unternehmen sich immer mehr zum Internet öffnen. Dies gilt nicht nur für das Bürokommunikationsumfeld, sondern auch für Fertigung und Produktion.

Wie weit die umfassende Vernetzung unterschiedlicher Systeme reicht, illustriert ein Blick in die Fabrik der Zukunft, die unter dem Schlagwort „Industrie 4.0“ firmiert. Mit dem Ziel, möglichst viele Informationen digital nutzbar zu machen, werden die „digitalertüchtigten“ Systeme des gesamten Unternehmens untereinander sowie nach innen und außen vernetzt: Die Maschinen, Sensoren und Feldgeräte in den Produktions-

anlagen, Enterprise-Resource-Planning(ERP)-Systeme, Marketing, Vertrieb und Einkauf. Auch entlang der Wertschöpfungskette wird die Vernetzung der IT-Systeme mit den Lieferanten, Kunden und Servicepartnern vorangetrieben. Dieser Trend wird die technologische Entwicklung in Unternehmen weiter maßgeblich gestalten. So werden bis 2020 in Deutschland im Bereich Industrie 4.0 Investitionen in Höhe von rund 11 Milliarden Euro erwartet.¹ Dieser Entwicklung kann sich kein Unternehmen entziehen, denn die über Industrie 4.0 zu erreichenden Effizienz- und Effektivitätssteigerungen müssen erlöst werden, will das Unternehmen nicht seine Wettbewerbsfähigkeit verlieren.

Als Folge der schnell voranschreitenden Digitalisierung und Vernetzung ergibt sich, dass der Schutz der IT-Netze und IT-Systeme an den Außengrenzen des Unternehmens immer weiter erodiert und sich neue Angriffsflächen eröffnen. Auch werden IT-Systeme angreifbar, die bislang aus dem Internet gar nicht erreichbar waren. Für die IT-Sicherheit ergibt sich daraus eine sehr viel komplexere Risikosituation. Perspektivisch vergrößert sich zunehmend auch das Risiko existenzgefährdender Situationen durch Ausfall oder Fehlfunktion von Produktions- oder Geschäftsprozessen.

Komplexität der IT

Die oben dargestellte Vernetzung aller Systeme und Dinge („Internet of Things“) sowie die Digitalisierung von physischen Systemen („Cyber-physical Systems“) steigert die Komplexität der digitalen Infrastrukturen in hohem Maße. Schon heute sind viele Haushaltsgeräte, Gebäudesteuerungen, Gefahren- und Brandmeldeanlagen, Verkehrssysteme und Automobile vernetzt und mit dem Internet verbunden. In Zukunft wird absehbar auch die digitale Stadt („Smart City“) realisiert werden.

Mit steigender Komplexität der Systeme stoßen altbekannte konventionelle IT-Sicherheitsmechanismen schnell an ihre Grenzen und vermögen es nicht, Zuverlässigkeit und Beherrschbarkeit im gewohnten Maße zu gewährleisten. Bereits jetzt ist der Bedarf für innovative Lösungsansätze zur Gewährleistung eines hinreichenden

IT-Sicherheitsniveaus der Gesamtsysteme sichtbar und wird in den kommenden Jahren noch weiter zunehmen.

Allgegenwärtigkeit durch Smartphones

Die Aspekte Innovation und Veränderung sind untrennbar mit der modernen Informationstechnologie verbunden. Für die Tragweite des seit einigen Jahren anhaltenden Smartphone-Booms gibt es jedoch auch in der IT-Branche bisher kaum vergleichbare Beispiele. Die Zahl der Smartphone- und Tablet-Nutzer wird mittlerweile in Milliarden gemessen und der Einfluss der Geräte auf das tägliche Leben ihrer Besitzer ist enorm. Das Smartphone ist dabei nicht die kabellose Fortschreibung der etablierten PC-Technologie, vielmehr handelt es sich hier um ein ganzes Bündel technologischer und konzeptioneller Aspekte, die in der Summe einen neuen, in sich abgeschlossenen Bereich der Informationstechnologie definieren. Die bisherigen Erkenntnisse und Verfahrensweisen zum Thema IT-Sicherheit sind hier nicht unmittelbar übertragbar und müssen überdacht und angepasst werden.

Ein besonderes Merkmal des Smartphones ist das „Always-On“, also die ständige breitbandige Verbindung zum Internet und die fortlaufende Aktivität des Gerätes auch ohne Interaktion des Nutzers. Die meisten Smartphones werden zudem von ihrem Besitzer ständig mitgeführt und protokollieren umfassend Aufenthaltsorte und Kommunikationsvorgänge, die zentral über dieses eine Gerät abgewickelt werden. Spätestens dann, wenn das Smartphone in Zukunft zur elektronischen Geldbörse wird, mit der man im Internet und über eine Funkschnittstelle auch direkt an Kasse bezahlen kann, stellt sich die Frage nach den grundsätzlichen Sicherheitskonzepten dieser mobilen Plattform und deren Wirksamkeit. In der Regel sind Anwender bei Smartphones darauf angewiesen, dass die Sicherheitsmechanismen des Betriebssystems greifen. Der Nutzer selbst kann nur sehr begrenzt individuelle Härtingsmaßnahmen umsetzen, die sich dann im Wesentlichen auf die sichere Konfiguration der Geräte beschränken.

Eine zentrale Rolle hinsichtlich der IT-Sicherheit spielt nicht nur das Endgerät, sondern auch das „ökonomische Gesamtsystem“, dem das jeweilige Smartphone zugeordnet ist. Hierzu zählt das jeweilige Betriebssystem, aber auch zahlreiche Hintergrundsysteme wie der App-Store, Downloadplattformen für Inhalte und cloudbasierte Backupssysteme des jeweiligen Anbieters sind relevant. Abgeschlossenheit und zentrale Verwaltung dieses „Ecosystem“ bieten zwar eine Grund-sicherheit, die in der traditionell offenen PC-Welt ohne zusätzliche Schutzmechanismen nicht erreicht wird, aber sie ist nicht transparent für den Nutzer, und eine Skalierbarkeit für höheren Schutzbedarf ist nicht vorgesehen. Als wichtiger Bestandteil der Gesamtökonomie des Systems liefert Sicherheit insofern erst die Grundlage für die gebündelte Vermarktung von Waren und Dienstleistungen und ist damit ein Hauptaugenmerk der Betreiber.

Unter den Erfolgsfaktoren der Produktkategorie Smartphone nimmt das Konzept der Apps eine herausragende Stellung ein. Hier erfolgte der eigentliche Quantensprung, da dem Nutzer mit dem Erwerb des Gerätes über Online-Marktplätze wie dem Apple App Store, Google Play oder dem Microsoft Windows Phone Store sofort auch der Zugriff auf Millionen von Anwendungsprogrammen ermöglicht wird.

Nicht nur die Beschaffung von Software, sondern auch der Schritt zum Softwareproduzenten sind hier so niederschwellig realisiert, dass mittlerweile über 100.000 Anbieter in den unterschiedlichen Online-Marktplätzen vertreten sind. Neben datenschutzrechtlichen Aspekten besteht auch aus der Perspektive der IT-Sicherheit bei Apps das größte Angriffspotenzial. Die Betriebssysteme selbst sind vergleichsweise gut gesichert, während die Möglichkeiten von Apps im Betriebssystem durch den Nutzer selbst bestätigt werden. Solche Berechtigungsabfragen sind aber weitgehend wirkungslos, weil diese Abfragen in den allermeisten Fällen unreflektiert durch den Nutzer bestätigt werden.

Allgegenwärtigkeit durch Clouds

Cloud-Services sind zentral über ein Netz und mit standardisierten Schnittstellen bereitgestellte Dienste zur Verarbeitung und Speicherung von Informationen. Sie verlagern Anwendungen, Rechenleistung und Speicherbedarf von (mobilen) Endgeräten in Cloud-Rechenzentren. Die wichtigsten Vorteile der Cloud-Services sind: Teils komplexe Funktionen werden wiederverwertbar an zentraler Stelle angeboten, die Pflege der Services ist einfacher und sie können leicht skaliert werden, Rechenleistung wird vom Endgerät ins Rechenzentrum verlagert. All dies kann zu erheblichen wirtschaftlichen Vorteilen führen.

Smartphones, Tablets und Apps bieten heute vielfältige Schnittstellen zu Cloud-Services des jeweiligen mobilen Systems und von Drittanbietern. Darüber kann unter anderem auch die Synchronisierung von Kontakten, Terminen, E-Mails, Fotos und Dokumenten mit anderen Endgeräten erfolgen. Somit werden auch zum Teil sehr persönliche Informationen in der Cloud gespeichert und verarbeitet. Dabei besteht jedoch keine Gewissheit, dass die Daten dort vor unrechtmäßigem Zugriff sicher und zudem dauerhaft abrufbar sind. In der Regel lehnen die Cloud-Anbieter über ihre allgemeinen Geschäftsbedingungen die Verantwortung für die hinterlegten Daten weitgehend ab.

Vor der Nutzung von Cloud-Services in Unternehmen sind daher von den Verantwortlichen einige Fragen zu klären: Welche Informationen eignen sich für die Verarbeitung und Speicherung in der Cloud und erlauben dies die Compliance-Anforderungen, insbesondere hinsichtlich des Datenschutzes. Immer mehr Cloud-Service-Provider drängen in den boomenden Markt und es ist nicht einfach, einen vertrauenswürdigen Anbieter zu identifizieren, der die eigenen Sicherheitsanforderungen erfüllt. Der Chance, von Skaleneffekten zu profitieren, steht ein Kontrollverlust über die eigenen Informationen gegenüber.

Ausblick

Für viele private Nutzer ist das Smartphone zum Dreh- und Angelpunkt für den Zugriff auf weltweite Informationen und Dienste geworden. Die Integration von Bezahl- und Gesundheitsfunktionen sowie Schnittstellen zur Heimautomation lässt künftig die Grenze zwischen der physischen und der virtuellen Welt zunehmend verschwinden. Fragen nach der Sicherheit mobiler Endgeräte und ihrer wirtschaftlichen Ökosysteme gewinnen somit verstärkt an Relevanz.

Im unternehmerischen Kontext sind aus dem Blickwinkel der IT-Sicherheit neben der Mobilität weitere Entwicklungen zu berücksichtigen. Die Nutzung von cloudbasierter Informationsverarbeitung verspricht einen Gewinn an Schnelligkeit und Kosteneinsparungen, stößt jedoch aus organisatorischen, technischen oder sicherheitstechnischen Gründen häufig noch auf Skepsis. Unternehmen mit industrieller Steuerungs- und Automatisierungstechnik sind zudem von der Konvergenz dieser Technik mit klassischer Informations- und Kommunikationstechnik, einschließlich mobiler Nutzung, betroffen. Dies bringt neue Herausforderungen hinsichtlich der IT-Sicherheit mit sich.

2 Gefährdungslage

2 Gefährdungslage

Mit der zunehmenden Digitalisierung und Vernetzung vieler Lebens- und Arbeitsbereiche geht eine dynamische Gefährdungslage einher. Ursachen von Cyber-Angriffen, Angriffsmethoden und die Nutzung der technischen Angriffsmittel entwickeln sich täglich weiter, hängen in vielfältiger Weise zusammen und beeinflussen sich gegenseitig.

2.1 Ursachen

Cyber-Angriffe auf Unternehmen, Verwaltungen und Privatanutzer kommen jeden Tag vor. Viele Angriffe verlaufen erfolgreich, weil die Angreifer zum einen immer professioneller werden und zum anderen auf Rahmenbedingungen treffen, die sie zu ihrem Vorteil zu nutzen wissen.

2.1.1 Angriffsplattform Internet

Die offene Struktur, die technischen Möglichkeiten und die Anonymität sind Ursachen dafür, dass das Internet als Angriffsplattform missbraucht wird. Dies spiegelt sich auch in der Masse der heutigen Cyber-Angriffe wider. Für erfolgreiche Cyber-Angriffe braucht man heute vielfach nicht mehr als einen PC und einen Internetanschluss. Diesen eher kleinen Investitionen stehen die vielfältigen Möglichkeiten gegenüber, durch kriminelle Handlungen Geld zu verdienen, vertrauliche Informationen zu erlangen oder Sabotageakte durchzuführen. Entsprechende Angriffswerkzeuge und -methoden sind einfach und kostengünstig verfügbar. Es existiert ein funktionierender globaler Markt, auf dem Angriffswerkzeuge, Schwachstellen, Schadsoftware oder sogar Webseiten-Traffic eingekauft oder als Dienstleistung beauftragt werden können („Malware-as-a-Service“). Auch die illegal erlangten Daten wie Nutzer-Accounts und Kreditkarteninformationen werden dort gehandelt. Es sind sowohl gut organisierte Gruppen als auch Einzelpersonen, die auf diesen kriminellen Online-Marktplätzen ihre Fähigkeiten und Dienstleistungen anbieten. Die Attraktivität des Internets als Angriffsplattform zeigt sich anhand der folgenden Randbedingungen, die die Angreifer für ihre Zwecke ausnutzen:

- Die zunehmende Vernetzung von Informationstechnik ermöglicht Angriffe aus der Distanz von nahezu jedem Ort der Welt und zu jedem Zeitpunkt auf immer mehr Ziele. Ein Angreifer muss

sich dadurch keinen unmittelbaren Risiken vor Ort aussetzen.

- Die zunehmende Komplexität der Technik und oftmals fehlendes Sicherheitsbewusstsein führen zu unzureichend abgesicherten Systemen und erhöhen damit die Erfolgsaussichten für Cyber-Angriffe.
- Der sorglose Informationsaustausch über das Internet und der „Always-On“-Status mobiler Systeme erleichtern den Zugriff auf schützenswerte Informationen.
- Das dezentral und offen gestaltete Internet bietet für Angreifer vielfältige Tarnungsmöglichkeiten, die das Risiko, entdeckt zu werden, minimieren.
- Unterschiede in nationalen Regularien erschweren Maßnahmen der Strafverfolgung.

Die Professionalisierung und Separierung unterschiedlicher Aufgaben im Bereich der Cyber-Kriminalität nimmt weiter zu. Ein Cyber-Angriff kann so arbeitsteilig von verschiedenen Personen oder Gruppen, die sich auf einzelne Schwerpunkte spezialisiert haben, unabhängig voneinander realisiert werden. So gibt es beispielsweise:

- Hacker, die neue Schwachstellen in weitverbreiteten Software-Produkten suchen und diese zum Verkauf anbieten.
- Entwickler, die zu diesen Schwachstellen passende Schadsoftware oder Werkzeuge zur Generierung von Schadsoftware entwickeln und anpassen.
- Angreifer, die diese Schadsoftware einsetzen, um Informationen auszuspionieren.
- Kriminelle, die die gestohlenen Informationen kaufen, ausnutzen und zu Geld machen.

So kann selbst ein unerfahrener Angreifer ohne technisches Know-how professionelle Angriffe auf gewünschte Ziele durchführen oder durchführen lassen, ohne sich mit technischen Details und der Ausführung befassen zu müssen.

2.1.2 „Digitale Sorglosigkeit“

Im Zuge der Medienberichte über die Snowden-Enthüllungen, über Cyber-Angriffe auf bekannte Wirtschaftsunternehmen und den damit verbundenen Abfluss von Kundendaten sowie über die Vorfälle von großflächigem Identitätsdiebstahl ist das Vertrauen vieler Anwender in die Informationstechnik erheblich erschüttert. Die Nutzer scheinen zunehmend für Themen der IT-Sicherheit sensibilisiert. So ermittelte eine Studie des Deutschen Instituts für Vertrauen und Sicherheit im Internet (DIVISI),² dass sich das Sicherheitsgefühl der Deutschen im Internet signifikant verschlechtert hat. Dieser Besorgnis steht ein weiterhin zu beobachtendes von scheinbarer Sorglosigkeit geprägtes Handeln gegenüber. Dies gilt sowohl in der geschäftlichen als auch in der privaten IT-Nutzung: Trotz erhöhter Sensibilisierung und schlechterem Sicherheitsgefühl werden konkrete Schutzmaßnahmen in der Praxis nur geringfügig häufiger umgesetzt. So ist beispielsweise die Verbreitung von E-Mail-Verschlüsselung nach wie vor gering.³ Lösungen sind verfügbar, entsprechen jedoch häufig nicht den Anforderungen der Anwender an Komfort, Intuitivität und Bedienbarkeit. Diese sind jedoch in vielen Fällen wesentliche Entscheidungsfaktoren für den Einsatz solcher Lösungen.

Komfort bzw. ein vorgeblich versprochener Nutzen sind auch die Anreize, die dazu führen, dass der Anwender selbst – durch Social Engineering getäuscht – persönliche Informationen preisgibt oder Schadsoftware ausführt. Täglich gibt es professionell gemachte Spam-Wellen und Versuche, über gefälschte Webseiten, E-Mails oder Kurznachrichten an persönliche Daten zu gelangen. Dabei werden häufig bekannte Unternehmen oder Institutionen als Absender missbraucht, um den Empfänger dazu zu bringen, auf einen Link oder einen Dateianhang zu klicken und so den Rechner mit Schadsoftware zu infizieren. Auch im Bereich der mobilen Kommunikation steht oft der Komfort im Vordergrund, wenn Anwender Smartphone-Apps ohne Überprüfung der Auswirkungen installieren und nutzen. Weiterhin sind auch Basis-Sicherheitsmaßnahmen wie ein wirksames Patch-Management, mit dem verfügbare Sicherheitsaktualisierungen von Programmen möglichst schnell eingespielt werden, noch immer nicht selbstverständlich.

Selbst wenn die Sensibilität für Gefährdungen vorhanden ist, werden angemessene Sicherheitsmaßnahmen nicht konsequent umgesetzt. Dies gilt außer für Privatanwender auch für kleine und mittelständische Unternehmen (KMU). So zeigt es sich, dass die Systeme der KMU⁴ – wie die Systeme der Bürger⁵ – häufig selbst gegen

einfache Angriffe nur unzulänglich geschützt sind. Das Niveau der Abwehr- und Schutzmaßnahmen der Netze und der zugehörigen Infrastrukturen in Deutschland ist allerdings unterschiedlich ausgeprägt: Die Netze einzelner Großunternehmen unterliegen in der Regel angemessenen Schutzmaßnahmen. Unternehmen sehen laut einer Umfrage der Allianz für Cyber-Sicherheit⁶ jedoch eine wachsende Gefahr durch Datenklauattacken und gezielte Angriffe durch Cyber-Kriminalität sowie staatliche Angreifer. Als Hauptursache für erfolgreiche Angriffe werden Softwareschwachstellen genannt. Ein Patch-Management ist jedoch nur bei knapp drei Vierteln der befragten Institutionen etabliert. Mehr als die Hälfte der befragten Unternehmen gaben an, dass ihre Maßnahmen zum Schutz vor Cyber-Angriffen aktuell nicht ausreichen und mittelfristig zusätzliche Maßnahmen geplant sind. Bedenklich ist, dass der Großteil der befragten Unternehmen der Umfrage zufolge weniger als fünf Prozent des gesamten IT-Budgets in die IT-Sicherheit investiert.

Neben allen technischen Schutzmaßnahmen ist auch das Verhalten des Anwenders mit entscheidend für einen hohen Grad an Sicherheit im Internet. Durch die zunehmende Komplexität und Mobilität der Informationstechnik wird es für Anwender wie auch für Hersteller und Dienstleister zunehmend wichtiger, die „digitale Sorglosigkeit“ abzulegen und sich frühzeitig und verantwortungsvoll mit Fragen der IT-Sicherheit zu befassen und entsprechende Lösungen im praktischen Handeln umzusetzen.

2.1.3 Schwachstellen

Schwachstellen sind Grundlage für die Entwicklung von Cyber-Angriffsmitteln und Ursache für erfolgreiche Cyber-Angriffe. Wie bereits in den Vorjahren war die Anzahl kritischer Schwachstellen in Standard-IT-Produkten auch in den Jahren 2013 und 2014 hoch. Allein in 13 Softwareprodukten, die weit verbreitet genutzt werden (Tabelle 1), traten 705 kritische Schwachstellen im Jahr 2013 auf. Für 2014 rechnet das BSI mit mehr als 700 kritischen Schwachstellen (Abbildung 1). Schwachstellen sind immanenter Bestandteil heutiger Software. Die Entwicklung fehlerfreier Software ist faktisch nicht oder nur in sehr eingeschränkten Spezialbereichen möglich. Allein für die Gruppe der weit verbreitet genutzten Produkte muss mit einer Erkennung von durchschnittlich zwei kritischen Schwachstellen pro Tag gerechnet werden.

Aufgrund der Masse an Schwachstellen ist das Patch-Verhalten der Hersteller von besonderer

Bedeutung. Diese sind zunehmend gezwungen, eine Priorisierung bei der Beseitigung von Schwachstellen vorzunehmen und sich auf kritische Schwachstellen zu konzentrieren.

Details zu Schwachstellen werden häufig erst nach Herausgabe eines Sicherheitsupdates („Patch“) durch den Softwarehersteller bekannt. Daher ist eine rasche Einspielung dieser Softwareaktualisierungen zwingend erforderlich. Falls Details oder gar Exploits, die eine bestimmte Schwachstelle ausnutzen, vor dem Patch des Softwareherstellers an die Öffentlichkeit gelangen (Zero-Day-Exploits), ist bei einem Einsatz der betroffenen Software höchste Vorsicht geboten. 2014 gab es bis Ende Juli fünf öffentlich bekannte Vorfälle dieser Art.

Softwareprodukte

- Adobe Flash Player
- Adobe Reader
- Apple OS X
- Apple Quicktime
- Apple Safari
- Google Chrome
- Linux Kernel
- Microsoft Internet Explorer
- Microsoft Office
- Microsoft Windows
- Mozilla Firefox
- Mozilla Thunderbird
- Oracle Java/JRE

Tabelle 1: Auswahl von Softwareprodukten mit hoher Relevanz

Ungepatchte Systeme sind nicht nur im Desktopbereich ein Problem, sondern betreffen in gleicher Weise auch den Server- und Mobilbereich: So gab es im Februar 2014 weltweit sechs Millionen Webseiten,⁸ die die veraltete, leicht angreifbare Version 1.3 der Serversoftware Apache verwendeten. Im Mobilbereich sind insbesondere auf Android-Geräten häufig veraltete Betriebssystemversionen anzutreffen.⁹ Viele Hersteller von Endgeräten stellen die Aktualisierungen nur für eine kurze Zeitspanne bereit. Spätestens mit Erscheinen des jährlichen Nachfolgemodells wird die Unterstützung älterer Versionen eingestellt. Neu entdeckte Sicherheitslücken werden dann nicht mehr gepatcht und stellen somit eine Gefahr für ältere Geräte dar.

Generell gilt: Softwareprodukte, bei denen der Produktsupport ausgelaufen ist, sollten nicht mehr betrieben werden, da für diese Produkte in der Regel auch keine Sicherheitsaktualisierungen mehr erfolgen. Aktuelles Beispiel ist Microsoft Windows XP, dessen erweiterter Produktsupport im April 2014 endete. Seit diesem Zeitpunkt gibt es für Windows XP weder funktionelle noch Sicherheitsupdates. Dennoch lag der Marktanteil von Windows XP in Deutschland Mitte des Jahres noch bei über acht Prozent, weltweit bei mehr als 15 Prozent.¹⁰

2.1.4 Einsatz veralteter Software und ungepatchter Systeme

Das Einspielen von Softwareaktualisierungen ist eine Grundvoraussetzung für ein sicheres IT-System. Veraltete Patchstände von Betriebssystemen und Applikationen sind dennoch eines der Hauptprobleme, die bei Audits und Penetrationstests des BSI in Behörden festgestellt werden. Auch viele Systeme von Privatanwendern sind nicht immer auf dem aktuellen Stand.

Trotz der gängigen Empfehlung, Auto-Update-Funktionalitäten zu nutzen, haben in Deutschland nach Erkenntnissen von IT-Experten mindestens zehn Prozent aller eingesetzten Windows-Betriebssysteme und anderer gängiger Softwareprodukte veraltete Patchstände.⁷ Diese Zahl ist als untere Grenze anzusehen.

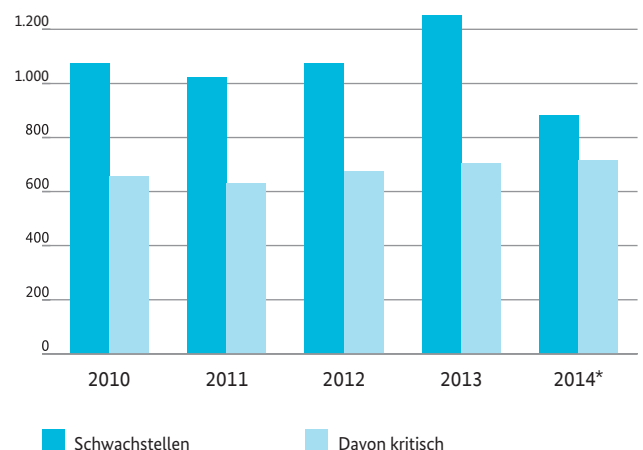


Abbildung 1: Anzahl aller Schwachstellen der gelisteten Softwareprodukte

*Die Werte für das Jahr 2014 wurden auf Basis der ermittelten Anzahl der Schwachstellen bis September hochgerechnet.

Typische Sicherheitsmängel

Das BSI führt regelmäßig Sicherheitsprüfungen wie Penetrations-tests oder IS-Revisionen bei Behörden durch. Zu den im Rahmen der Überprüfungen am häufigsten auftretenden Sicherheitsmängeln gehören:

- » Patchstände von Betriebssystemen und Applikationen sind veraltet und verfügbare Sicherheitsmechanismen deaktiviert.
- » Passwörter sind – auch bei kritischen Anwendungen – leicht zu ermitteln. Nicht selten werden Standardpasswörter, leere oder andere schwache Passwörter verwendet.
- » Maßnahmen zu Netzwerkmanagement und -überwachung sind nicht oder lediglich als Insellösungen existent, Logdaten werden lediglich lokal auf den Komponenten selbst vorgehalten und nur anlassbezogen manuell ausgewertet.
- » Eine Netzwerkzugangskontrolle (auch für Wartungszugänge und -verbindungen), die ausschließlich autorisierten dienstlichen Endgeräten den Zugang zum internen Netzwerk ermöglicht, wird oftmals nicht genutzt.
- » Es existiert keine Schnittstellenkontrolle für mobile Datenträger und mobile Endgeräte werden nicht verschlüsselt.
- » Änderungen an Anwendungen und Betriebssystemen werden ohne angemessenes Änderungs- und Versionsmanagement in den Produktivbetrieb eingestellt und größtenteils nicht dokumentiert.
- » Schulungen und Sensibilisierungsmaßnahmen finden insbesondere für die Zielgruppe der Anwender nicht oder nur in geringfügigem Umfang statt.
- » Die Verantwortlichkeit für Informationssicherheit durch die Unternehmens- oder Behördenleitung bzw. das Management ist oftmals nicht klar geregelt.
- » Sicherheitskonzepte sind unvollständig und inkonsistent.

2.1.5 Mobile Endgeräte

Klassische Desktop- und Laptop-Rechner werden zunehmend durch Smartphones und Tablets ergänzt und ersetzt. Mobile Endgeräte stellen ein lohnendes Angriffsziel dar, da sie üblicherweise das komplette „digitale Leben“ des Besitzers widerspiegeln – von E-Mails über Social Media bis hin zu Flugtickets, Online-Banking oder Standortinformationen. Neben den Gefahren durch Verlust und Diebstahl gibt es besondere Herausforderungen bezüglich der IT-Sicherheit in Bezug auf Betriebssystemaktualisierungen und Apps. Bedingt durch eine rasante Entwicklung im Hardwarebereich werden die Aktualisierungen von Software oftmals nur für eine kurze Zeitspanne bereitgestellt, sodass Sicherheitslücken nicht mehr behoben werden. Eine weitere Gefahr besteht in der unüberschaubaren Masse von verfügbaren Apps, die nicht selten Schad- und Spionagefunktionen enthalten. Hiervon ist Android, bedingt durch seinen offenen Ansatz, vermehrt betroffen.

Gerade bei der Nutzung mobiler Endgeräte möchte man jederzeit und an jedem Ort auf seine Daten zugreifen können. Somit werden auch teils sehr persönliche Informationen in einer Cloud gespeichert. Falls der Zugriff auf die Cloud nicht ausreichend geschützt ist, sind diese Informationen stark gefährdet. Dies zeigt unter anderem ein aktueller Vorfall, bei dem intime Fotos von Prominenten aus der iCloud entwendet und im Internet veröffentlicht wurden.

Die Bedrohung mobiler Geräte nimmt ständig zu

Die Anzahl der Schadprogramme für mobile Endgeräte steigt nach Berichten aller Hersteller von Antivirensoftware kontinuierlich an. Zusätzlich zu etablierten Angriffsmethoden, die auch im PC-Bereich Anwendung finden, eröffnen die mobilen Geräte durch ihre „Always-On“-Eigenschaft weitere Angriffsmöglichkeiten:

» Infektion mit Schadprogrammen durch Apps

Apps können neben vorgeblich nützlichen Funktionen auch Schadfunktionen enthalten. So gibt es Trojaner, die sich als nützliche Apps tarnen, im Hintergrund jedoch Informationen ausspionieren oder auf Kosten des Besitzers teure SMS-Nachrichten versenden bzw. unerwünschte Anrufe tätigen.

» Nutzung öffentlicher Hotspots

Die meisten öffentlichen Hotspots bieten keine Verschlüsselung. Die Daten werden offen übertragen und können somit von unbefugten Dritten mitgelesen werden. Insbesondere betroffen hiervon können Online-Banking oder die Übertragung vertraulicher Informationen sein.

» Überwachung und Datenabfluss

Der Aufenthaltsort von Mobilfunkgeräten – und damit auch ihrer Besitzer – kann von den Betreibern der Funknetzwerke, von den App-Anbietern, aber auch von Cyber-Kriminellen, die Zugriff auf das Gerät haben, jederzeit ermittelt werden. Durch die Überwachung der Smartphones und den Diebstahl von Informationen wie Passwörtern, Bildern, Logdateien oder GPS-Koordinaten kann ein umfassendes Profil der Opfer erstellt werden.

» Abhören von Telefonaten

Das Telefonieren über GSM (Standard zur mobilen Sprach- und Datenübertragung) ist nicht abhörsicher. Schützenswerte oder geheime Informationen können hierdurch an Dritte abfließen.

2.1.6 Unzureichende Absicherung industrieller Steuerungssysteme

Systeme zur Fertigungs- und Prozessautomatisierung – zusammengefasst unter dem Begriff Industrial Control Systems (ICS) – werden in nahezu allen Infrastrukturen eingesetzt, die physische Prozesse abwickeln. Ein Trend im Zuge der Entwicklung zu Industrie 4.0 ist die erweiterte Vernetzung dieser industriellen Steuerungssysteme über die internen Netze eines Unternehmens hinweg. Dadurch

halten IT-Komponenten immer stärker Einzug in die eigentlichen Produktionsnetze, um so industrielle Abläufe im globalen Ausmaß effizienter und effektiver zu gestalten. Viele dieser Systeme wurden jedoch nicht im Hinblick auf mögliche Angriffe konzipiert.

Bedrohungen für Steuerungskomponenten in Industrie und produzierendem Gewerbe

Systeme zur Fertigungs- und Prozessautomatisierung sind zunehmend Cyber-Angriffen ausgesetzt. Die Betreiber müssen das Risiko und Schadenspotenzial sowohl von nichtzielgerichteter Schadsoftware als auch von gezielten, qualitativ hochwertigen und mit signifikantem Aufwand durchgeführten Angriffen gegen ICS-Infrastrukturen berücksichtigen.

Die zentralen Bedrohungen, denen ICS derzeit ausgesetzt sind:¹¹

- 1 Infektion von Steuerungskomponenten mit Schadsoftware über Büronetze
- 2 Einschleusen von Schadsoftware über Wechseldatenträger und externe Hardware
- 3 Social Engineering
- 4 Menschliches Fehlverhalten und Sabotage
- 5 Einbruch über Fernwartungszugänge

Neben Angriffen, die durch Fehler bei der Softwareimplementierung zum Erfolg führen, spielt das Social Engineering eine immer größer werdende Rolle. Bei dieser Methode führen meist nichttechnische Handlungen zu unberechtigtem Zugang zu Informationen oder IT-Systemen. Dabei werden menschliche Eigenschaften wie Hilfsbereitschaft, Neugier, Vertrauen oder Angst ausgenutzt. Daher sind Maßnahmen wie Sensibilisierung und Schulung auch im Bereich von ICS ein wesentlicher Baustein für mehr Sicherheit.

Bei der Betrachtung der wichtigsten Bedrohungen im Kontext industrieller Steuerungssysteme wird zudem deutlich, dass zu den zentralen Erfolgsfaktoren und Rahmenbedingungen für die Realisierung und die Akzeptanz von Industrie 4.0 die Entwicklung von IT-Sicherheitskonzepten, -architekturen und -standards gehören.

2.2 Angriffsmittel und -methoden

Die Mittel und Methoden für Cyber-Angriffe sind heute sehr vielfältig. Sie werden in unterschiedlicher Art und Weise eingesetzt und kombiniert, um Cyber-Angriffe sowohl in der Breite als auch für zielgerichtete Angriffe gegen Einzelpersonen oder Institutionen einzusetzen. Das vorliegende Kapitel liefert einen Einblick in die heute genutzten Angriffsmethoden und enthält Lageinformationen und Bewertungen.

2.2.1 Spam

Als Spam bezeichnet man unerwünschte Nachrichten, die massenhaft und ungezielt per E-Mail oder über andere Kommunikationsdienste versendet werden. In der harmlosen Variante enthalten Spam-Nachrichten meist unerwünschte Werbung. Häufig enthält Spam jedoch auch Schadprogramme im Anhang, Links zu Webseiten mit Drive-by-Exploits oder wird für Phishing-Angriffe genutzt. Für den Versand von Spam-Nachrichten sind umfangreiche Ressourcen wie Botnetze oder kompromittierte Server notwendig.

Lage

- Im Jahr 2014 zeichnet sich mit dem deutlichen Zuwachs von ca. 80 Prozent im Vergleich zum Vorjahr eine Trendwende bei den seit Jahren stagnierenden Spam-Zahlen ab (siehe Abb. 2).
- Deutschland liegt in den weltweiten Top Ten der Spam-Versender im Mittelfeld.
- 2014 ist im Vergleich zum Vorjahr ein Anstieg von E-Mails mit Schadsoftware im Anhang um 36 Prozent zu verzeichnen.
- Seit Anfang 2014 ist ein Trend zur pseudozufälligen Generierung von Varianten der Schadsoftware während des Versands zu beobachten.
- Kriminelle versenden zunehmend Office-Dokumente als Anhang, über deren Makros Schadprogramme nachgeladen werden.
- Als Folge von Identitätsdiebstahl erfolgt Spam-Versand vermehrt über kompromittierte Nutzerkonten etablierter E-Mail-Dienste.

Bewertung

Als lange bekanntes Phänomen lässt sich die Masse an Spam-Nachrichten heute mit Gegenmaßnahmen wie Spam-Filtern oder Greylisting grundsätzlich reduzieren. Aus betrieblicher Sicht ist Spam daher heute weitestgehend unproblematisch. Qualität und Quantität von Schadprogramm-Spam steigen jedoch weiter an. Einmal verwendete Varianten von Schadcodes erhöhen den Aufwand in der Analyse und verlangsamen die Bereitstellung passender Abwehrmaßnahmen wie Signaturen für Virenschutzprogramme.

2.2.2 Schadprogramme

Schadprogramme sind Werkzeuge, über die ein Angreifer Kontrolle über ein infiziertes System ausüben kann. Es gibt verschiedene Typen von Schadprogrammen, bspw. Viren, Trojanische Pferde (Trojaner), Bots oder Rootkits. Dabei sind Schadprogramme heute vielfach nicht mehr eindeutig zu kategorisieren, da sie modular aufgebaut sind und eine Vielzahl unterschiedlicher Schadfunktionen mitbringen oder auch nachladen können. Neben der klassischen PC/Notebook-Plattform sind heute zunehmend auch Mobilplattformen wie Smartphones und Tablets von Schadprogrammen betroffen.

Lage

- Schätzungen zufolge übersteigt die Gesamtzahl der PC-basierten Schadprogrammvarianten inzwischen die 250-Millionen-Marke.
- In Deutschland gibt es jeden Monat mindestens eine Million Infektionen durch Schadprogramme.
- Die Zahl der Schadprogrammvarianten steigt täglich um rund 300.000.

- Die häufigsten Verbreitungswege von Schadprogrammen sind Drive-by-Exploits, Anhänge in Spam-Mails sowie Botnetze.
- Die am häufigsten detektierten Schadprogrammtypen sind Adware und Trojaner.
- Mit etwa 95 Prozent ist vorwiegend das Betriebssystem Microsoft Windows von Schadprogrammen betroffen.
- Mobile Plattformen: Die Gesamtzahl der Schadprogramme für mobile Geräte wie Smartphones und Tablets liegt bei mindestens drei Millionen. 98 Prozent davon betreffen das Betriebssystem Android.
- Schadprogramme für mobile Plattformen werden meist als legitime App getarnt. Sie werden in der Regel nicht über offizielle App-Stores wie Google Play, sondern vorwiegend über alternative App-Stores oder Webseiten verbreitet oder vom Nutzer selbst unwissentlich installiert.
- Die Angreifer professionalisieren den Einsatz von Schadprogrammen, etwa durch verbesserte Methoden, um Steuerungsserver zu verstecken, durch die Nutzung von Twitter-Kanälen oder Google-Docs als Command-and-Control(C&C)-Server sowie durch den Einsatz aktueller Verschlüsselungsverfahren (beispielsweise Elliptische-Kurven-Kryptographie) zur Absicherung der Kommunikation.
- Neben den klassischen Schadprogrammen, über die Daten abfließen oder Online-Banking manipuliert wird, ist auch die „Ransomware“, die Zugriff auf Systeme blockiert oder Nutzerdaten verschlüsselt, um so ein Lösegeld zu erpressen, ein alltäglich von Cyber-Kriminellen eingesetztes Mittel geworden.

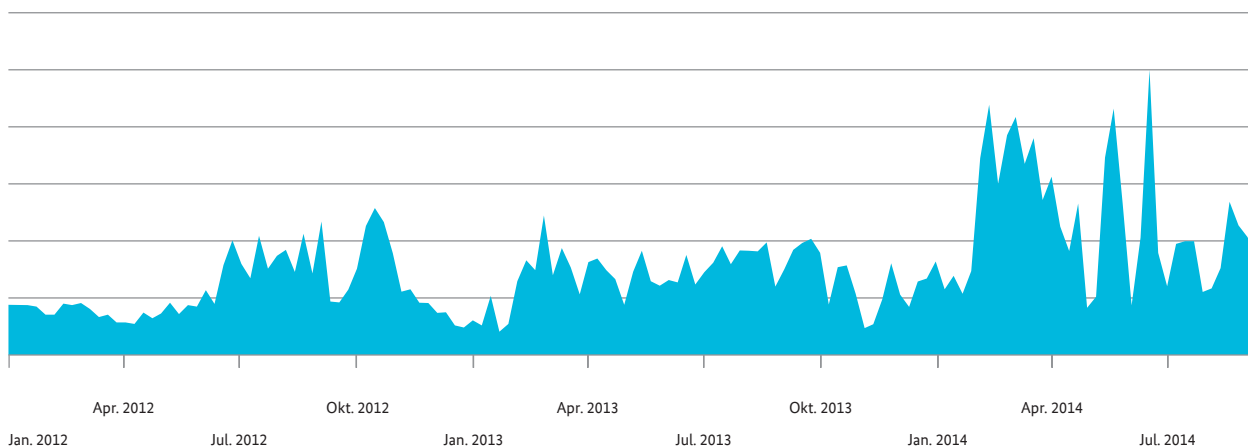


Abbildung 2: Qualitativer Spam-Verlauf pro Woche in Deutschland seit Januar 2012

Bewertung

Aufgrund der Masse und Komplexität von neuen Schadprogrammen reicht die Zeitspanne, bis neue Schadprogramme von Virenschutzprogrammen erkannt werden, von einigen Stunden bis hin zu mehreren Tagen. In diesem Zeitraum ist ein System ggf. ungeschützt. Klassische signaturbasierte Komponenten von Virenschutzprogrammen stoßen dadurch zunehmend an die Grenzen ihrer Wirksamkeit, wodurch eine Fortentwicklung der Schutzmaßnahmen notwendig wird. Weiterhin betreiben die Entwickler der Schadprogramme viel Aufwand, um mit immer neuen Methoden eine manuelle Analyse von Schadprogrammen und Vorfällen durch Analysten und Forensiker zu erschweren.

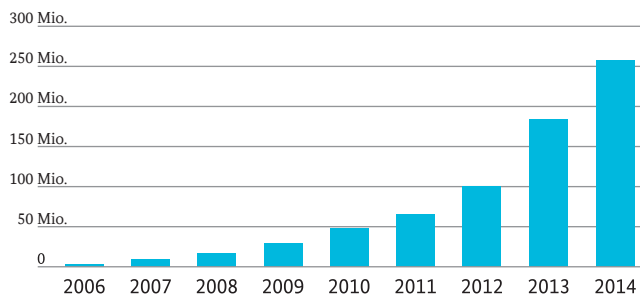


Abbildung 3: Anzahl Windows-Schadsoftwarevarianten

2.2.3 Drive-by-Exploits und Exploit-Kits

Der Begriff Drive-by-Exploit bezeichnet die automatisierte Ausnutzung von Sicherheitslücken durch den Besuch einer präparierten Webseite. Dabei werden ohne Benutzerinteraktion Schwachstellen im Browser, in Plug-ins oder im Betriebssystem ausgenutzt, um Schadprogramme unbemerkt auf dem System des Webseitenbesuchers zu installieren. Besonders effizient arbeiten Drive-by-Exploits in sogenannten Exploit-Kits: Statt eines einzelnen Exploits kommen darin mehrere Exploits zum Einsatz, die automatisiert versuchen, eine Schwachstelle im Browser oder in dessen Plug-ins zu finden und zur Installation von Schadprogrammen zu verwenden. In sogenannten Watering-Hole-Angriffen werden Drive-by-Exploits für gezielte Angriffe verwendet.

Lage

- Drive-by-Exploits werden auf massenhaft oder gezielt kompromittierten verwundbaren Webseiten platziert.
- Laut einer Auswertung der Google Safe-Browsing-Daten¹² lag der Anteil von Webseiten mit Drive-by-Exploits oder anderer Verbreitung von Schadsoftware in den letzten zwölf Monaten in Deutschland bei vier Prozent.
- Die Angriffe durch Exploit-Kits richteten sich in den letzten Monaten am häufigsten gegen Schwachstellen im Internet Explorer. Auch Oracle Java ist weiterhin ein beliebtes Angriffsziel, wenn auch nicht mehr so im Fokus wie noch 2013.

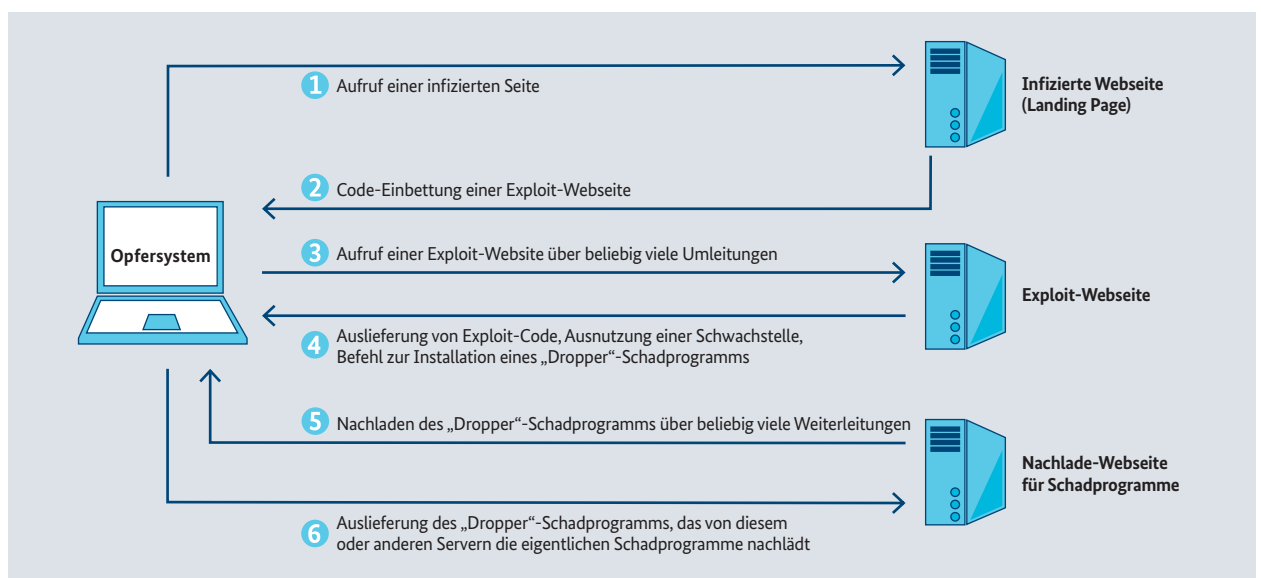


Abbildung 4: Beispiel einer Schadprogramminfektion per Drive-by-Exploit

Bewertung

Exploit-Kits spielen eine zentrale Rolle bei Cyber-Angriffen mit kriminellem Hintergrund. Ein Exploit-Kit, das in eine beliebte Webseite eingebunden ist, infiziert in kürzester Zeit eine Vielzahl verwundbarer Systeme ohne Kenntnis oder Mitwirken des Benutzers. Bei dieser breiten bzw. ungezielten Angriffsmethode werden die Opfersysteme mit unterschiedlichen Schadprogrammen infiziert, beispielsweise Ransomware zum Erpressen von Geld, Trojanische Pferde zum Identitätsdiebstahl und -missbrauch sowie Bots zum Aufbau einer Infrastruktur für den Versand von Spam oder für DDoS-Angriffe. Aktuell existiert für jede in Exploit-Kits genutzte Schwachstelle ein Sicherheitsupdate des jeweiligen Herstellers, weshalb sich Angriffe mittels Exploit-Kits durch ein effektives Patch-Management verhindern ließen. Die Verwendung von Zero-Day-Exploits im Zusammenhang mit Exploit-Kits ist selten.

Manipulierte Werbebanner

2013 wurden vom BSI über 350 in Deutschland gehostete kompromittierte OpenX-Server identifiziert, von denen schädliche Werbebanner auf Webseiten eingeblendet wurden. Der mit den Werbebannern ausgelieferte schädliche Code verwies auf Drive-by-Exploits. Potenziell gefährdet waren Besucher, die nicht die aktuellen Sicherheitsupdates für das Windows-Betriebssystem sowie Software wie Oracle Java, Adobe Reader oder Flash Player installiert hatten. Die Infektionen erfolgen beim Aufruf der Webseite unbemerkt und ohne Zutun des Benutzers – ein Anklicken des schädlichen Banners war nicht erforderlich.

Einige der OpenX-Server wurden von Medienagenturen betrieben, wodurch schädliche Banner auch auf populären Webseiten mit täglich vielen tausend Besuchern eingeblendet wurden. Das BSI hat die Betreiber der Webseiten bzw. der OpenX-Server sowie die zuständigen Provider über die Kompromittierungen informiert.¹³ Zum Teil war das mehrfach notwendig, da Betreiber zunächst nicht reagierten oder die Server nach Bereinigung erneut kompromittiert wurden.

Neben der Notwendigkeit einer raschen Installation von Sicherheitsupdates verdeutlicht dies erneut, dass die Gefahr von Infektionen mit Schadprogrammen über Werbebanner nicht nur in den Graubereichen des Internets geschehen kann, sondern auch auf populären, seriösen Webseiten.

2.2.4 Botnetze

Als Botnetz wird ein Verbund von Systemen bezeichnet, die von einer fernsteuerbaren Schadprogrammvariante (einem sogenannten Bot) befallen sind. Die betroffenen Systeme werden vom Botnetz-Betreiber mittels eines Command-and-Control-Servers (C&C-Server) kontrolliert und gesteuert. Botnetze werden von Kriminellen genutzt, um im großen Stil Informationsdiebstahl und Online-Banking-Betrug zu begehen, um Angriffe auf die Verfügbarkeit von Computersystemen durchzuführen (DDoS-Angriffe) oder um massenhaft Spam- und Phishing-Mails oder E-Mails mit weiteren Schadprogrammen im Anhang zu versenden.

Lage

- Nach Schätzungen sind allein in Deutschland mehr als eine Million Internetrechner Teil eines Botnetzes.
- Aufgrund der Professionalisierung und Kommerzialisierung der Aktivitäten im Bereich Cybercrime ist der Aufbau und Betrieb eines Botnetzes auch für technische Laien vergleichsweise einfach und kostengünstig.
- Informationsdiebstahl ist eines der größten Probleme im Zusammenhang mit Botnetzen. Neben klassischen Endnutzersystemen werden vermehrt auch internetfähige Geräte angegriffen, die Informationen wie beispielsweise Zahlungsdaten verarbeiten.
- Zunehmend werden auch Webserver kompromittiert und zu Botnetzen zusammengeschlossen. Aufgrund ihrer breitbandigen Netzanbindung und hoher Verfügbarkeit eignen sich diese Systeme zum Beispiel zur Ausführung von DDoS-Angriffen.

Bewertung

Wie aktuelle Meldungen zu Informationsdiebstählen und Online-Banking-Betrugsfällen durch Botnetze zeigen, ist die Lage als kritisch zu bewerten. Botnetz-Infrastrukturen bieten Internetkriminellen immense Ressourcen an Rechnerkapazität und Bandbreite, die sie für ihre kriminellen Handlungen einsetzen können. Heute sind überwiegend Windows-Systeme Teil eines Botnetzes. Aber auch Mac OS X und Android-Geräte rücken als Zielplattform für Botnetze zunehmend in den Fokus der Cyber-Kriminellen. Auch andere internetfähige Geräte wie DSL-Router oder Smart-TVs werden zum Ziel von Angriffen und Infektionen. Ein Grund hierfür sind die schwächeren Schutzmechanismen dieser Geräte. Vor dem Hintergrund des Trends zum Internet der Dinge wird dieser Aspekt an Bedeutung gewinnen.

2.2.5 Social Engineering

Bei Angriffen mittels Social Engineering versuchen Kriminelle, ihre Opfer dazu zu verleiten, eigenständig Daten preiszugeben, Schutzmaßnahmen zu umgehen oder selbstständig Schadcode auf ihren Systemen zu installieren. Sowohl im Bereich der Cyber-Kriminalität als auch bei der Spionage gehen die Täter geschickt vor, um menschliche Schwächen wie Neugier auszunutzen und so Zugriff auf sensitive Daten und Informationen zu erhalten.

Lage

- Der Trend, persönliche Daten und Informationen mittels eines Sozialen Netzwerks oder einer privaten Webseite verstärkt einer breiten Öffentlichkeit zugänglich zu machen, erleichtert es den Kriminellen, diese Informationen zur Vorbereitung von Social Engineering bei gezielten Angriffen zu verwenden.
- Kriminelle nutzen regelmäßig die menschliche Neugier auf interessante Informationen, das Interesse an Schnäppchen, die Vorsicht oder das schlechte Gewissen bei behördlichen Benachrichtigungen oder strafrechtlichen Androhungen sowie die erhöhte Aufmerksamkeit bei Großereignissen wie der Fußball-WM, zu Feiertagen oder bei aktuellen wirtschaftlichen oder gesellschaftlichen Themen (zum Beispiel SEPA-Umstellung) aus.
- Phishing-Angriffe, bei denen E-Mails mit gefälschtem Absender verschickt und Nutzer dadurch zur Preisgabe ihrer persönlichen Informationen verleitet werden sollen, gibt es weiterhin in großer Anzahl. Die vorgeblichen Absender sind bekannte Unternehmen und Organisationen, Finanzdienstleister sowie bekannte Online-Shops, E-Mail- oder Kommunikationsanbieter. Mit fiktiven Bestellungen, Rechnungen, Mahnungen oder auch Sicherheitshinweisen werden Nutzer auf gefälschte Webseiten verwiesen, um dort Zugangsdaten, Kontoinformationen oder sonstige Kundendaten zu aktualisieren oder zu bestätigen.
- Bei einem besonders aufwendigen Angriff auf deutsche Konzerne erhielten Mitarbeiter E-Mails, die angeblich von Mitarbeitern der Personalabteilung stammen sollten. Mit aufwendig gefälschten Mailhistorien und angeblichen Vorstandsentscheidungen wurden die Empfänger aufgefordert, ihre Stamm- und Kontodaten u.ä. zu schicken. Mit den Daten nahmen die Täter Kontoauflösungen oder Neubestellungen von EC-Karten vor.
- Beim Online-Banking werden Nutzer mit manipulierten Testüberweisungen oder Nutzerverifikationen (TAN, mTAN) dazu gebracht, Daten in

gefälschte Web-Formulare einzutragen oder angebliche Sicherheits-Apps zu installieren, hinter denen sich Schadprogramme verbergen. Die vorgeblichen Webseiten der Banken sind inzwischen kaum mehr als Nachbildung zu erkennen.

- Social Engineering ist elementarer Bestandteil gezielter Angriffe.

Bewertung

Technische Maßnahmen erhöhen das IT-Sicherheitsniveau, können aber allein keinen vollständigen Schutz gewährleisten. Dies zeigt sich besonders deutlich bei Angriffen mittels Social Engineering. Solange Anwender unbedarft private Informationen preisgeben oder unbedarft eine E-Mail mit einem vermeintlich verlockenden kommerziellen Angebot anklicken, werden Kriminelle Social Engineering nutzen, um mit den gewonnenen Daten einen finanziellen Gewinn zu erzielen. Da Social Engineering auch häufig Einfallstor für gezielte Angriffe auf Unternehmen und Behörden ist, sind Sensibilisierung und Schulungen der Mitarbeiter unerlässlich. Das Beispiel Phishing verdeutlicht, wie wichtig ein umsichtiger Nutzer für die Datensicherheit ist.

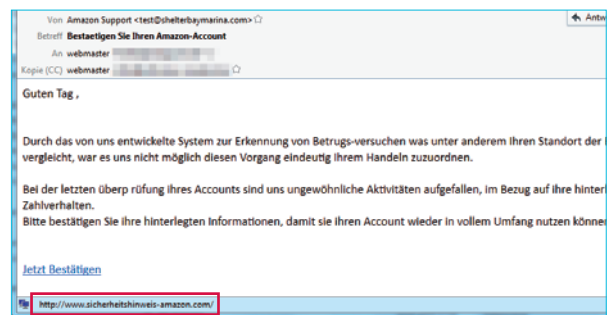


Abbildung 5: Beispiel einer Phishing-Mail – erkennbar an der gefälschten Absenderadresse

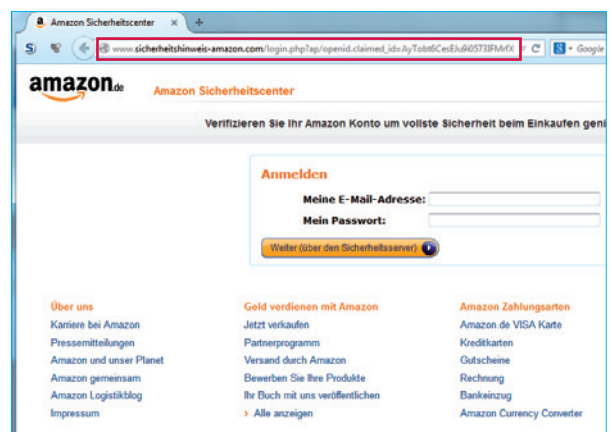


Abbildung 6: Beispiel einer Phishing-Webseite – erkennbar an der gefälschten URL

2.2.6 Identitätsdiebstahl

Als Identitätsdiebstahl oder -missbrauch bezeichnet man die Aneignung und unberechtigte Nutzung personenbezogener Daten wie Anschrift, E-Mail-Adresse, Geburtsdatum, Bankkonto- oder Kreditkartennummern durch Dritte. Ziel eines Angreifers ist es in der Regel, finanzielle Vorteile durch vertrauliche Informationen zu erlangen, in selteneren Fällen auch den rechtmäßigen Identitätsinhaber in Misskredit zu bringen. Identitätsdiebstahl findet vor allem mittels Social Engineering, Schadprogrammen auf infizierten Systemen oder durch Datenabfluss nach dem Hacking von Online-Angeboten statt.

Lage

- Identitätsdiebstahl ist ein alltägliches Phänomen: Jeden Monat wird eine große Zahl an digitalen Identitäten allein von infizierten Rechnern von Privatanwendern gestohlen.
- Die Anzahl der Schadprogramme für Identitätsdiebstahl steigt kontinuierlich an. Allein das BSI analysiert monatlich rund 11.000 Schadprogramme, die einen Bezug zu Identitätsdiebstahl in Deutschland haben.
- Mittlerweile setzen Täter gezielt Schadsoftware ein, die auf bestimmte Daten spezialisiert ist, etwa auf digitale Identitäten, die mit hoher Wahrscheinlichkeit auch missbraucht werden können (z.B. aus den Bereichen Online-Banking oder -Shopping).
- Im Frühjahr 2014 informierte das BSI über zwei große Vorfälle von Identitätsdiebstahl: Insgesamt sind dabei rund 34 Millionen digitale Identitäten in Form von E-Mail-Adressen und Passwörtern abgeflissen.
- Auch Angriffe auf Diensteanbieter sind attraktiv: Bereits heute ist die Zahl der entwendeten Identitäten durch Angriffe auf Server von Online-Anbietern oder -Dienstleistern wesentlich höher als die Zahl der Identitätsdiebstähle über die Rechner von Internetnutzern. Ein Angriff auf die Handelsplattform eBay im Mai 2014 beispielsweise betraf weltweit 145 Millionen Kunden, davon ca. 15 Millionen in Deutschland.

Bewertung

Die Cyber-Bedrohung durch Identitätsdiebstahl wird weiter steigen, solange den professionell aufgestellten Angreifern viele unzureichend geschützte Systeme von Anwendern und Diensteanbietern gegenüberstehen. Passwort-Management sowie das regelmäßige Einspielen aller

relevanten Systemupdates können mit geringem Aufwand einen wichtigen Beitrag zum Schutz persönlicher Daten liefern. Auch Online-Diensteanbieter sind in der Pflicht, bessere Schutzmaßnahmen für ihre Systeme und die Daten ihrer Kunden zu ergreifen. So sollte es selbstverständlich sein, Kundendaten bzw. entsprechende Datenbanken ausschließlich verschlüsselt vorzuhalten. Zudem sollten den Anwendern sichere Authentifizierungsverfahren wie die Zwei-Faktor-Authentifizierung angeboten werden. Möglich ist dies beispielsweise auch mit dem neuen Personalausweis, den mittlerweile Millionen von Bundesbürgern besitzen.

2.2.7 Denial of Service

Denial-of-Service(DoS)-Angriffe richten sich gegen die Verfügbarkeit von Diensten, Webseiten, einzelnen Systemen oder ganzen Netzen. Wird ein solcher Angriff mittels mehrerer Systeme parallel ausgeführt, spricht man von einem verteilten DoS- oder DDoS-Angriff (DDoS = Distributed Denial of Service). DDoS-Angriffe erfolgen häufig durch eine sehr große Anzahl von Computern. Dies können zu einem Botnetz zusammengesetzte, kompromittierte Systeme oder auch wissentlich zusammengeschaltete Rechner von freiwilligen Teilnehmern sein, wie beispielsweise bei politisch motivierten Angriffen. Hinter DDoS-Angriffen auf große Unternehmen und Regierungen stehen oft eher politische oder ideologische Motive, bei Angriffen auf E-Commerce-Anbieter geht es vermehrt um Wettbewerbsbeeinflussung oder Erpressung. DDoS-Angriffe werden mit zunehmender Häufigkeit auch gegen KRITIS-Betreiber wie Banken, Transportunternehmen und Medienunternehmen eingesetzt. Auch hier verfolgen die Täter bislang in erster Linie finanzielle Interessen, etwa durch Erpressungsversuche.

Lage

- Im Jahr 2014 gab es allein in Deutschland bisher über 32.000 DDoS-Angriffe.
- Nahezu alle Branchen sind von DDoS-Angriffen betroffen.
- Im Rahmen einer Umfrage der Allianz für Cyber-Sicherheit¹⁴ haben mehr als ein Drittel der befragten Unternehmen angegeben, in den letzten drei Jahren Ziel eines DDoS-Angriffes auf ihre Webseiten gewesen zu sein.
- Ein Viertel der befragten Unternehmen war von DDoS-Angriffen auf die Netzinfrastruktur betroffen.

- Seit 2013 treten verstärkt sogenannte Reflection-Angriffe auf. Dabei wird nicht das Zielsystem direkt angegriffen, sondern es werden offene zur Verfügung stehende Dienste im Internet (DNS¹⁵ oder NTP¹⁶) missbraucht. Ein Angreifer schickt im Namen des Opfers Anfragen an einen solchen offenen Dienst. Die Dienste schicken ihre Antworten dann an das Opfersystem. Da die Antworten in der Regel sehr viel größer als die Anfragen sind, können bereits wenige Angreifersysteme großen Schaden anrichten und das Opfersystem lahmlegen. Bei Reflection-Angriffen werden unbeteiligte Parteien wie die Dienstebetreiber ungewollt zu Mittätern.
- Im Februar 2014 wurde der bisher stärkste derartige DDoS-Angriff mit 400 Gigabit pro Sekunde verzeichnet. Dieser Angriff basierte auf NTP-Reflection.
- Die Anzahl der NTP-Server in Deutschland, die sich für diese Art von Angriff ausnutzen lassen, ist im Zeitraum von Juni 2014 bis August 2014 von über 4.000 Systemen auf rund 2.500 gesunken. Grund hierfür ist die Information der betroffenen Betreiber durch das BSI.

Bewertung

Im weltweiten Vergleich ist die Betroffenheit in Deutschland geringer als in anderen Ländern. Insgesamt ist Deutschland weder als Quelle noch als Ziel von Angriffen besonders auffällig. Dennoch kann ein DDoS-Angriff für ein betroffenes Unternehmen ein existenzielles Problem darstellen.

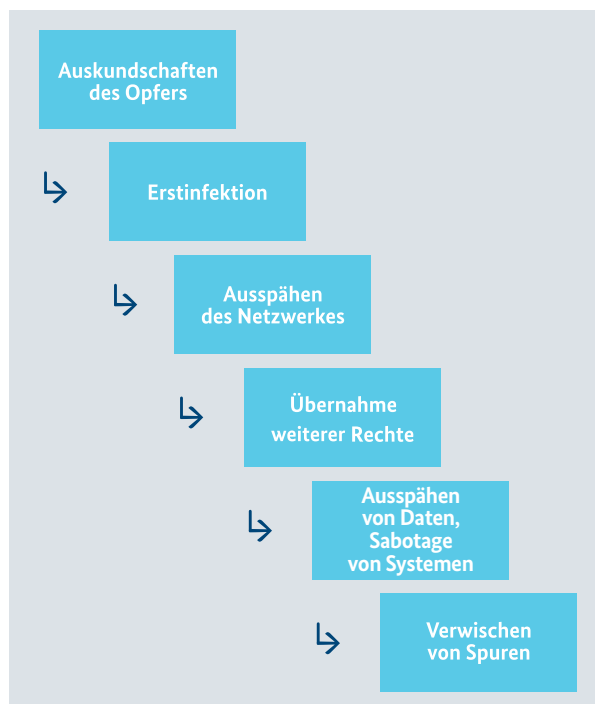


Abbildung 7: Vorgehensweise bei einem APT-Angriff

2.2.8 Advanced Persistent Threats (APT)

Bei Advanced Persistent Threats handelt es sich um zielgerichtete Cyber-Angriffe auf spezifisch ausgewählte Institutionen und Einrichtungen, bei denen sich ein Angreifer persistenten Zugriff zu einem Opfernnetzwerk verschafft und in der Folge auf weitere Systeme ausweitet. Die Angriffe zeichnen sich durch einen sehr hohen Ressourceneinsatz und erhebliche technische Fähigkeiten aufseiten der Angreifer aus und sind in der Regel schwierig zu detektieren.

Lage

- Im Fokus von APT-Angriffen stehen vorrangig die Rüstungsindustrie, Hochtechnologiebranchen wie Automobilbau, Schiffsbau und Raumfahrt, Forschungseinrichtungen sowie die öffentliche Verwaltung.
- Die Erstinfektion erfolgt bei APT-Angriffen häufig durch den Empfang einer E-Mail mit präpariertem Dokumentenanhang und zielgerichtetem Social Engineering. Durch die Verwendung plausibler oder erwarteter Informationen aus dem beruflichen Umfeld sowie der Nennung eines vertrauenswürdigen Absenders ist eine Unterscheidung zwischen authentischer und gefälschter Nachricht bei zielgerichtetem Social Engineering häufig nicht möglich.
- Ein weiterer Trend zur Initiierung von APTs sind Watering-Hole-Angriffe. Dabei wird zunächst eine von der Zielperson häufig genutzte Webseite kompromittiert. Besucht die Zielperson dann diese Webseite, wird der Rechner mittels eines Drive-by-Exploits mit einem Schadprogramm infiziert. Alternativ wird dem Opfer eine E-Mail mit Link auf die präparierte Seite zugeschickt. Der mittels Social Engineering erstellte Inhalt der E-Mail verleitet den Empfänger dazu, auf den Link zu klicken.
- Angriffe verlaufen häufig zunächst über wenig technikaffine Zielpersonen im Unternehmen.
- Besonders bei größeren Organisationen wird meist die zentrale Verzeichnisstruktur angegriffen. In der nächsten Phase des Angriffs werden Daten exfiltriert oder Zielsysteme sabotiert. Der Angreifer versucht, die Systeme des Opfers möglichst lange unter seiner Kontrolle zu behalten, ohne dass das Opfer auf ihn aufmerksam wird. In der Praxis hat sich gezeigt, dass fortlaufende APTs über mehrere Monate bis Jahre unentdeckt blieben. In der letzten Phase des APT-Angriffs werden vorhandene Spuren bestmöglich verwischt.

Bewertung

APT-Angriffe sind eine ernstzunehmende Bedrohung für die deutsche Wirtschaft und die öffentliche Verwaltung. Das Hacking von schlecht gesicherten Unternehmensservern wird künftig weiter an Bedeutung gewinnen. Für die frühzeitige Warnung potenziell gefährdeter Unternehmen sowie die Erstellung eines umfassenden Lagebildes ist es unerlässlich, die Vorgehensweise und die Angriffswerkzeuge bei APT-Angriffen noch exakter auszuwerten. Die Meldung von Vorfällen an das BSI durch betroffene Unternehmen liefert dazu einen wichtigen Beitrag.

2.2.9 Nachrichtendienstliche Cyber-Angriffe

Deutschland ist permanent Cyber-Angriffen ausgesetzt, die darauf zielen, informative und finanzielle Vorteile zu erlangen. Verbesserte technische Sensorik des BSI in den Regierungsnetzen, aber auch die Auswertung der Enthüllungen von Edward Snowden haben technisches Wissen und Verständnis über nachrichtendienstliche Cyber-Angriffe sowie Cyber-Angriffsmethoden im Laufe der Jahre 2013/2014 erweitert.

Die verbesserte technische Sensorik des BSI lieferte verstärkte und deutliche Hinweise auf nachrichtendienstliche Cyber-Angriffe gegen deutsche Netzinfrastrukturen der Wirtschaft, der Forschung und der öffentlichen Verwaltung. Dies wurde auch von Partnerbehörden und Partnern des BSI in der Wirtschaft beobachtet. Nicht zuletzt auch aus den Snowden-Veröffentlichungen ergibt sich ein deutlicher Erkenntniszugewinn. So überraschen die Snowden-Enthüllungen hinsichtlich Professionalität, Ausmaß und Dichte nachrichtendienstlicher Überwachungsmaßnahmen sowie des erheblichen Ressourcenaufwandes, sowohl personell als auch finanziell.

Eine genauere Analyse der vorliegenden technischen Erkenntnisse lässt vier mögliche Hauptangriffsvektoren erkennen:

- **Angriffsvektor „Strategische Aufklärung“:**
Es werden alle anfallenden Daten an Internet- und Kommunikationsknoten abgegriffen, gespeichert und analysiert. Hierbei sind die (Verkehrs-) Daten beliebiger Internetnutzer betroffen, anhand derer festgestellt werden kann, wer mit wem zu welchem Zeitpunkt an welchem Ort kommuniziert hat. Sind die Inhalte unverschlüsselt, so sind auch diese in vollem Umfang mithörbar, etwa bei Telefonaten über VoIP. Gleiches gilt für Daten bei Internetserviceprovidern wie etwa Soziale Netzwerken oder Suchdiensten.

- **Angriffsvektor „Individuelle Angriffe im Kommunikations- und Cyber-Raum“:**
Diese Angriffe zielen auf IT-Systeme interessanter Personen und Institutionen. Dazu analysieren, kaufen und sammeln Nachrichtendienste bereits im Vorfeld systematisch vor allem auch bis dahin nicht veröffentlichte Schwachstellen von Hard- und Software. In der strategischen Aufklärung identifizierte IT-Systeme werden dann auf dieser Wissensbasis mit spezifisch adaptierten Cyber-Angriffen attackiert und kontrolliert. Auch Funk- und Mobilkommunikation können durch entsprechende Angriffe individuell belauscht werden. Auf diese Weise können Computer einzelner Nutzer mit Schadsoftware angegriffen und danach von jedem Ort der Welt aus in Echtzeit überwacht werden. Wird ein Smartphone durch die Zielperson genutzt, kann diese getrackt werden, d. h., ihr Aufenthaltsort kann ständig ermittelt werden und in vielen Fällen kann durch strategische Aufklärung ein Gesprächspartner identifiziert werden, der ebenfalls ein Smartphone oder Notebook bei sich trägt.
- **Angriffsvektor „Beeinflussung von Standards und Implementierungen“:**
Hierbei werden bereits im Vorfeld der technischen Aufklärung IT-Standards und vor allem kryptografische Standards manipuliert. Die Implementierungen an sich starker Sicherheitsmechanismen und die hiermit verbundene Vertraulichkeit werden so systematisch geschwächt. Dies bedeutet, dass die heute international standardisierten, starken Kryptoalgorithmen in Hard- oder Softwareimplementierungen zum Beispiel mit schwachen Zufallsgeneratoren kombiniert werden und damit keinen ausreichenden Schutz der Vertraulichkeit mehr bieten.
- **Angriffsvektor „Gezielte Manipulation von IT-Equipment“:**
Hierbei erfolgen Eingriffe in Bestell-, Liefer- oder Serviceketten, um Manipulationen durchzuführen. Hierzu zählen das Einbringen von Hintertüren oder die Schwächung technischer Sicherheitseigenschaften. So werden etwa Monitore, Tastaturen oder Video- und Audiokabel mit Miniatursendern versehen, die eine Erfassung des Funksignals auch aus größerer Entfernung ermöglichen. Netzwerkkomponenten wie Router können durch Änderung ihrer Betriebssoftware so manipuliert werden, dass eine Steuerung oder gar Abschaltung aus der Ferne und damit auch Cyber-Sabotage möglich wird.

Beispielhaft für diese Angriffsvektoren sind die Angriffsszenarien gegen Mobilkommunikation, die das folgende Schaubild verdeutlicht.

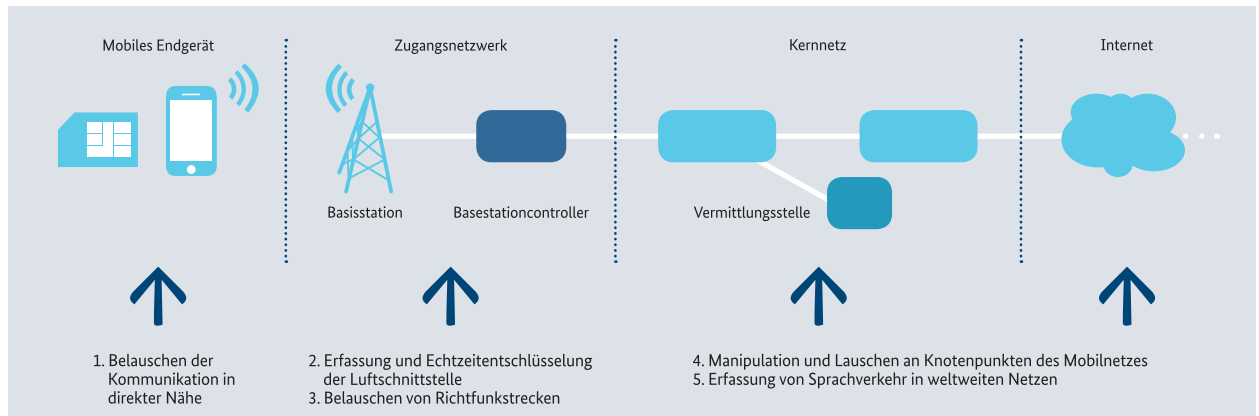


Abbildung 8: Angriffsvektoren auf Mobilkommunikation

Alle dargestellten Möglichkeiten, IKT-Systeme zum Zwecke von technischer oder Cyber-Spionage zu kompromittieren, können auch in gleicher oder ähnlicher Weise genutzt werden, um Cyber-Sabotage zu verüben. Dies trifft in besonderem Maße auf die in Kritischen Infrastrukturen eingesetzte Informations- und Kommunikationstechnologie zu.

2.3 Angreifer-Typologie

Trotz der großen Anzahl unterschiedlicher Angriffsziele und möglicher Angriffsmethoden kann die Motivation hinter einem Cyber-Angriff häufig auf finanzielle Interessen, Informationsbeschaffung, Sabotage, Einflussnahme oder die Durchsetzung politischer Interessen zurückgeführt werden. Generell können drei Angreifertypen unterschieden werden: Kriminelle, Nachrichtendienste und Hacktivisten. Eine Besonderheit bilden Innentäter.

2.3.1 Cyber-Kriminelle

Einleitung

Die Motivation von Cyber-Kriminellen ist es, mithilfe der Informationstechnik auf illegalen Wegen Geld zu verdienen. Organisierte Cyber-Kriminalität reicht vom Identitätsdiebstahl mit Warenbetrug über den Diebstahl von Geld durch Missbrauch von Bankdaten bis hin zur Erpressung. Organisierte Cyber-Kriminelle nutzen die genannten Vorteile von Cyber-Angriffen bei ihren Aktivitäten mit hoher Professionalität aus. Neben der organisierten Kriminalität gibt es auch Einzeltäter oder kleinere Gruppen, die sich jedoch meist durch geringere Professionalität in ihrer Vorgehensweise auszeichnen.

Fähigkeiten

Die Methoden und Varianten Cyber-Krimineller orientieren sich sowohl am technischen Fortschritt als auch an den bestehenden Abwehrmaßnahmen. Die Angreifer nutzen dabei die gesamte Bandbreite der technischen Möglichkeiten aus. Bei Privatanwendern sind das Spam- und Phishing-Mails, Schadsoftware zum Identitätsdiebstahl oder Manipulation von Online-Banking, Adware, Scareware sowie der Einsatz von Ransomware. Über unseriöse Jobangebote werden Privatpersonen unbeabsichtigt zu Finanz- oder Warenagenten und somit unwissend Teil von Finanz- und Warenbetrug.

Zu den verbreiteten Angriffsszenarien auf Unternehmen gehören unterschiedliche Formen der Erpressung oder das Hacking von Serverdiensten. Schadprogramme werden verstärkt in Kassensysteme (Point of Sale, POS) eingeschleust, um bei Bezahlvorgängen die Kundendaten direkt vom Kassensystem mitzulesen.

Kriminelle bieten darüber hinaus gegen entsprechende Bezahlung auch Cyber-Spionage und die Ausforschung von Wettbewerbern an. Mithilfe der Konkurrenzausspähung können interne Informationen über Mitbewerber und deren Produkte geldwerte Vorteile im globalen Wettbewerb bedeuten.

Ziele

Cybercrime ist heute allgegenwärtig. Alle Anwendergruppen – Wirtschaft, Wissenschaft, Verwaltung und Bürger – sind davon betroffen. Solange Kriminelle die Möglichkeit haben, auf diesem Weg Geld zu verdienen, werden sie diese nutzen und ihre Methoden weiterentwickeln.

Im Bundeslagebild Cybercrime 2013 des Bundeskriminalamtes (BKA) werden über 64.000 Fälle für das Jahr 2013 genannt. Gleichzeitig geht das BKA

von einem großen Dunkelfeld aus.¹⁷ Laut einer Umfrage der Allianz für Cyber-Sicherheit sind Cyber-Kriminelle die Angreifergruppe mit dem höchsten Bedrohungspotenzial in den kommenden Jahren.

Ransomware

Digitale Erpressung mittels Ransomware, die den Zugriff auf infizierte Systeme sperrt oder Nutzerdaten verschlüsselt, ist auch in Deutschland weit verbreitet. Das BSI-Service-Center wird regelmäßig von betroffenen Bürgerinnen und Bürgern kontaktiert, die Opfer eines Ransomware-Angriffs geworden sind und Hilfeleistung suchen. 2014 gab es bisher knapp 1.200 Anfragen, 2013 waren es mehr als 8.500 Anfragen. Seit Anfang 2014 gibt es mehrere neue Ransomware-Varianten, die mit verbesserten Methoden ausgestattet sind und Nutzersysteme oder Server infizieren und verschlüsseln können. Inzwischen existieren auch erste Varianten für Angriffe auf Android-Smartphones. Kommt ein Opfer der Erpressung nach, entsteht ein direkter Geldtransfer vom Opfer zum Täter, was Ransomware aus Tätersicht attraktiv macht. Dafür werden anonyme Bezahlungssysteme wie Guthaben- und Wertkarten oder sogenannte Kryptowährungen genutzt. Der Zwischenschritt mittels Warenbetrug oder Finanzagenten entfällt. Das BSI empfiehlt Betroffenen, den geforderten Geldbetrag keinesfalls zu zahlen, sondern stattdessen den befallenen Rechner zu bereinigen und ggf. Strafanzeige bei der Polizei zu stellen.

2.3.2 Nachrichtendienste

Einleitung

Cyber-Angriffe durch staatliche Nachrichtendienste dienen heute primär der Spionage und Wirtschaftsspionage.¹⁸ Im militärischen Sektor wird der Cyber-Raum inzwischen vielfach als weitere wichtige Domäne neben den klassischen militärischen Feldern Land, See, Luft und Weltraum angesehen.

Fähigkeiten

Die Fähigkeiten von staatlichen Nachrichtendiensten im Cyber-Raum sind lediglich durch den Ressourceneinsatz beschränkt, auch wenn dieser zum Teil immens ist. Nachrichtendiensten stehen als staatlichen Organisationen vielfältige Methoden zur Verfügung: Zugriff auf zentrale Infrastrukturkomponenten oder deren Betreiber, Eingriffe in die IT-Produkte ab Werk oder der Einbau von Hintertüren in Produkte über den Hersteller im eigenen Land. Klassische Cyber-Angriffe, beispielsweise mittels Trojanern, werden gezielter eingesetzt und haben eine höhere Qualität als die Kampagnen der Cyber-Kriminellen. Neben Standard-Tools und -vorgehensweisen kommen eigenständig oder von Dienstleistern entwickelte spezialisierte Schadprogramme zum Einsatz.

Nachrichtendienste können zudem weiterhin viel Geld in die Suche nach Schwachstellen investieren, um diese dann auszunutzen. Da in Abhängigkeit von der Größe und Qualität einer Software immer mit einer bestimmten Anzahl von Schwachstellen zu rechnen ist, stehen stets neue Einfallstore für Cyber-Angriffe zur Verfügung.

Ziele

Die Ziele von Angriffen durch Nachrichtendienste sind Unternehmen in Schlüsselindustrien und Kritischen Infrastrukturen sowie Regierungseinrichtungen, Verwaltung und Forschung anderer Staaten. Je nach Hintergrund werden Spionage- und Sabotageangriffe mit der Absicht ausgeführt, eigenen staatlichen Interessen zu dienen oder nationalen Wirtschaftsunternehmen Vorteile auf den internationalen Märkten zu verschaffen. Aufgrund der umfassenden Fähigkeiten können heute Wirtschaft, Verwaltung und Bürger gleichermaßen gezielt oder unbeabsichtigt Ziel von nachrichtendienstlichen Aktivitäten werden. Der Qualität dieser Angriffe kann nur durch einen hohen Aufwand bei der Umsetzung von Abwehrmaßnahmen begegnet werden.

2.3.3 Haktivismus und Cyber-Aktivisten

Einleitung

Im Bereich des Haktivismus angesiedelte Angriffe nutzen Computersysteme und Netzwerke vorgeblich als Protestmittel, um politische oder ideologische Ziele zu erreichen. Haktivisten wollen durch ihre Aktionen auf gesellschaftliche, soziale, wirtschaftliche oder technische Missstände aufmerksam machen, die ihrer Meinung nach bestehen. Sie vergleichen diese Form des Protests oft mit konventionellen Protestformen wie Demonstrationen, Aktivismus oder zivilem Ungehorsam. Für die angegriffenen Organisationen entstehen durch Haktivismus jedoch unter Umständen reale Schäden.

Fähigkeiten

Die Haktivisten-Szene ist heterogen und umfasst mehrere Gruppen, in denen einzelne Gruppierungen oder auch einzelne Haktivisten zusammengefasst werden können, beispielsweise die Anonymous-Bewegung, die Enthüllungsplattformen oder Cyber-Occupier. Haktivisten agieren häufig anlassbezogen und organisieren sich sehr schnell. Haktivisten sind in der Lage, DDoS-Angriffe, Webseiten-Manipulationen sowie gezielte Desinformation mittels Sozialer Netzwerke durchzuführen. Weiterhin werden gezielt Daten gestohlen und veröffentlicht, um einer bestimmten Forderung öffentliche Aufmerksamkeit zu verschaffen. Nicht selten finden

Aktivitäten durch Haktivisten parallel zu konventionellen Protestaktionen statt.

Ziele

Aufgrund der Motivation stehen hauptsächlich Staaten, staatliche Organisationen und große Wirtschaftsunternehmen im Fokus von Haktivisten. Die aktuelle Bedrohungslage in Deutschland ist insgesamt niedrig. Die internationale Bedrohungslage ist hingegen kritisch einzuschätzen, da es eine erhöhte Anzahl von Vorfällen gab, auch in KRITIS-Bereichen wie Informations- und Kommunikationstechnologie (IKT), Ernährung, Medien und Kultur.

2.3.4 Innentäter

Neben den drei genannten Angreifertypen gibt es mit Innentätern eine weitere Tätergruppe, die für Angriffe auf firmeninterne oder vertrauliche Informationen sowie Sabotage in Frage kommt. Durch den im Vergleich zu externen Angreifern weniger eingeschränkten Zugang zu internem Know-how und Ressourcen ist die Erfolgswahrscheinlichkeit für den unbemerkten Abfluss von unternehmenskritischen Daten und Informationen durch Innentäter besonders hoch einzuschätzen. Zudem können etablierte Schutzmaßnahmen vom Innentäter über einen langen Zeitraum analysiert und somit leichter überwunden werden. Darüber hinaus nutzen Innentäter das ihnen entgegengebrachte Vertrauen in der eigenen Organisation aus. Neben Mitarbeitern können auch externe Dienstleister zu Innentätern werden, die durch ihre Tätigkeit Einfluss oder direkten Zugang zu internen Informationen oder Prozessen haben.

2.4 Zusammenfassung

Die aktuelle IT-Landschaft und die vielfältigen Facetten der aktuellen Gefährdungslage sind eine permanente Herausforderung für Anwender von Informationstechnik. Heute existiert eine Vielzahl von Ursachen und Rahmenbedingungen, die die Durchführung von Cyber-Angriffen begünstigt. Die stetige Weiterentwicklung und Professionalisierung der Angreifer und ihrer Angriffsmethoden führen ebenfalls zu einer erhöhten Bedrohungslage für die Informationssicherheit.

Tabelle 2 fasst die Gefährdungslage der Angriffsmethoden und -mittel zusammen. Die Lage der IT-Sicherheit in Deutschland ist im Hinblick auf das daraus ersichtliche Angriffspotenzial als kritisch zu bewerten.

Zentrale Ursachen und Bedrohungen für Privatanwender

Mit Blick auf die Gefährdungslage sind die Systeme von Privatanwendern aktuell von den folgenden Ursachen und Bedrohungen besonders betroffen:

- 1** Unzureichendes Patch-Management und Nutzung veralteter Software auf allen Endgeräten
- 2** Cyber-Angriffe mittels Spam-Mails mit Schadcode im Anhang und Social Engineering, bei dem Anwender mittels vorgeblichen Rechnungen, Bestellbestätigungen oder Abmahnungen dazu verleitet werden, ein Schadprogramm auszuführen
- 3** Cyber-Angriffe über kompromittierte Webseiten oder manipulierte Werbefbanner, die beim Besuch einer Webseite Schadprogramme installieren
- 4** Cyber-Angriffe auf Diensteanbieter mit der Folge von Datenabfluss von Kundendaten
- 5** „Digitale Sorglosigkeit“ im Umgang mit mobilen Endgeräten und Apps sowie Preisgabe persönlicher Informationen

Zentrale Ursachen und Bedrohungen für Wirtschaft und Staat

Von vielen der heute gängigen Bedrohungen sind sowohl Bürger als auch Wirtschaft und Staat als Anwender von Informations- und Kommunikationstechnik gleichermaßen betroffen. Das gilt insbesondere für ungezielte Angriffe wie Spam-Mails oder Drive-by-Angriffe über kompromitierte Webseiten oder Werbebanner. Aufgrund der höheren Komplexität in geschäftlichen Umgebungen und des anzunehmenden höheren Sicherheitsniveaus im Vergleich zu Privatanwendern sind die zentralen Bedrohungen und Ursachen dennoch unterschiedlich:

- 1** Gezielte Spionage-Angriffe auf Wirtschaftsunternehmen, Forschung und Staat, die mit zielgerichtetem Social Engineering, unbekannten Schwachstellen und speziell entwickelten Tools durchgeführt werden
- 2** Cyber-Angriffe auf Unternehmenswebseiten oder Dienstangebote
- 3** Unzureichende Absicherung vernetzter industrieller Steuerungssysteme in Industrie und produzierendem Gewerbe
- 4** Herausforderungen durch Integration mobiler Endgeräte („Bring Your Own Device“) und externer Dienstleister in bestehende IKT-Infrastrukturen
- 5** Unzureichendes Patch-Management und Nutzung veralteter Software auf allen Endgeräten

Die Einschätzung der Bedrohung wird durch Analysen und Veröffentlichungen der Hersteller von Virenschutzprogrammen und IT-Sicherheitsdienstleistern untermauert: Die Experten sind sich darüber einig, dass vermehrte Angriffe mittels Ransomware, ein starker Anstieg bei Schadprogrammen für mobile Betriebssysteme sowie die Zunahme von gezielten Angriffen zu den aktuellen Topbedrohungen zählen.

Hohe Dunkelziffer

Über die bekannte Bedrohungslage hinaus muss zusätzlich mit einem großen Dunkelfeld gerechnet werden. Auch diese Lageeinschätzung basiert auf der Beobachtung und Analyse eines Ausschnitts der tatsächlichen Lage in Deutschland und weltweit. Vorfälle, die vielfach nicht gemeldet werden, erschweren eine realistische Einschätzung der Lage. Eine Studie zur Wirtschaftsspionage¹⁹ kommt zu dem Ergebnis, dass nur bei rund einem Viertel der Vorfälle externe Experten oder staatliche Stellen einbezogen wurden. Meldungen an Polizeien oder Staatsanwaltschaften erfolgten sogar nur in fünf Prozent der Fälle. Aufschlussreiche Informationen über Angriffsmethoden, verwendete Werkzeuge und Ziele bzw. Rückschlüsse auf Täter und ihre Motivation verbleiben so regelmäßig im Unklaren.

Die Vorfälle im nachfolgenden Kapitel zeigen, zu welchen Auswirkungen Schwachstellen, Schadprogramme oder eine unvollständige Absicherung in der Vergangenheit geführt haben. Die Vorfälle sind Beispiele dafür, wie sich eine vornehmlich abstrakte Bedrohung für Institutionen oder Einzelpersonen binnen kürzester Zeit in konkrete Risiken und reale Schäden auswirken kann.

Bedrohungen	2013	2014	Prognose
Schwachstellen	↑	→	→
Spam	↓	↑	→
Schadprogramme	↑	↑	↑
Drive-by-Exploits und Exploit-Kits	↑	→	→
Botnetze	→	→	→
Social Engineering	→	↑	→
Identitätsdiebstahl	↑	↑	↑
Denial of Service (DoS; DDoS)	→	→	→
Advanced Persistent Threats (APT)	↑	→	↑

↑ Steigend → Gleichbleibend ↓ Sinkend

Tabelle 2: Zusammenfassung der Gefährdungslage der Angriffsmethoden und -mittel

3 Vorfälle

3 Vorfälle

Anfang des Jahres 2014 konnten zwei millionenfache Diebstähle von digitalen Identitäten aufgedeckt werden, die eine Zäsur markierten. Spätestens seit diesen Vorfällen sind die aktuelle Lage der Bedrohung von IT sowie Cyber-Angriffe in den Fokus des politischen und medialen Interesses gerückt. Neben den genannten Identitätsdiebstählen verdeutlichen auch die hier ausgewählten Vorfälle eindrucksvoll die inzwischen perfektionierte, flexible und aufwendige Vorgehensweise der Angreifer. Im Fokus der Angriffe stehen dabei alle Gruppen von IT-Anwendern: Unternehmen, Behörden, Forschungseinrichtungen, Bürger und KRITIS-Betreiber. Besonders schwerwiegend sind Vorfälle bei Letzteren, da Beeinträchtigungen durch Cyber-Angriffe hier schnell gravierende Folgen für Bevölkerung und Wirtschaft und damit für das Gemeinwohl haben können.

3.1 Vorfälle in der Bundesverwaltung

Das BSI-Lagezentrum ist zentrale Meldestelle für IT-Sicherheitsvorfälle in der Bundesverwaltung. Seit 2010 müssen die Behörden gravierende Sicherheitsvorfälle unverzüglich und weniger kritische Vorfälle monatlich an das Lagezentrum übermitteln. Das BSI kann dadurch neben der unmittelbaren Reaktion auf den aktuellen Angriff auch Trends und Entwicklungen im Hinblick auf die Bedrohungslage für die IT und Netze der Bundesverwaltung ableiten und entsprechend frühzeitig Maßnahmen ergreifen.

Der Schutz von Systemen und Kommunikation der Bundesverwaltung basiert auf einem mehrstufigen Sicherheitsmodell. Neben gängigen Virenschutzprogrammen kommen weitere Schutzmaßnahmen an unterschiedlichen Schnittstellen zum Einsatz, mit denen in Echtzeit schädliche E-Mails abgewehrt werden können. Seit Mai 2014 wurden mit der damit verbundenen Vorgehensweise monatlich bis zu 60.000 verseuchte E-Mails in den Netzen der Bundesverwaltung zusätzlich abgefangen. Um hochwertige Angriffe abwehren zu können, setzt ein weiteres System auf die Erkennung von Angriffen, die gängige Schutzmechanismen bereits überwunden haben. 2014 wurden bisher täglich etwa 15 bis 20 Angriffe auf das Regierungsnetz entdeckt, die durch normale Schutzmaßnahmen nicht erkannt worden wären. Bei durchschnittlich einem Angriff pro Tag handelt es sich um einen gezielten Angriff mit nachrichtendienstlichem Hintergrund. Eine weitere Schutzstufe besteht in der Blockie-

rung nach außen gehender Kommunikationsverbindungen. Der Internetverkehr wird daraufhin überprüft, ob er zu bekannten Kontrollservern für Botnetze oder Spionageprogramme Verbindungen aufbaut. Diese Verbindungen aus dem Regierungsnetz können direkt blockiert und an die zuständige Behörde gemeldet werden, damit der infizierte Rechner bereinigt werden kann. So werden täglich rund 3.500 Zugriffe auf Schadcodeserver blockiert. Seit Anfang des Jahres 2014 wurden 34 infizierte Systeme identifiziert, die trotz Absicherung durch kommerzielle IT-Sicherheitsprodukte mit Schadprogrammen kompromittiert worden waren. Es wurden ca. 1.100 Webseitenbetreiber vom BSI darüber informiert, dass ihre Webseiten Schadprogramme verteilen.

Das BSI verzeichnet durchschnittlich einmal im Monat einen Denial-of-Service(DoS)-Angriff auf einzelne Webseiten der Bundesbehörden. In den an das BSI aus der Bundesverwaltung gemeldeten Fällen ging es unter anderem auch um die Ausnutzung von Schwachstellen in Webanwendungen. So versendeten Angreifer in mehreren Fällen jeweils zwischen 20.000 bis hin zu 200.000 Spam-Nachrichten, indem sie das Ausfüllen des „Weiterleiten“-Formulars per Skript automatisierten und den Spam-Inhalt in das Kommentarfeld einfügten. Die in diesem Fall verwundbare „Seite empfehlen“-Funktion der Behörden-Webseite wurde daraufhin dauerhaft deaktiviert bzw. um Schutzmaßnahmen ergänzt.

Bei einem anderen Angriff erhielten über 900 Mitarbeiter per E-Mail den Link einer auf die Behörde zugeschnittenen Phishing-Webseite. In der E-Mail wurde vorgegeben, dass die Speichergrenze des E-Mail-Postfachs überschritten und der Empfang weiterer E-Mails nicht mehr möglich sei. Um wieder E-Mails empfangen zu können, sei die Bestätigung des E-Mail-Kontos erforderlich. Auf der Phishing-Webseite wurden E-Mail-Adresse, Benutzername und Passwort abgefragt. Mit Bekanntwerden des Angriffs wurde der Zugriff auf die verlinkte Phishing-Webseite gesperrt.

Auch Vorfälle, die nicht auf einen Cyber-Angriff zurückzuführen sind, haben großen Einfluss auf die Verfügbarkeit einer IT-Infrastruktur und damit auf die IT-Sicherheit. Nach Auswertung weiterer Meldungen, die das Lagezentrum aus der Bundesverwaltung erhält, wird deutlich, dass Störungen oder Ausfälle bei Strom- und Klimaanlagen in Rechenzentren oftmals nicht durch

die vorgesehenen Notstromverfahren abgedeckt werden und zu stundenlangen Störungen führen können. Eine weitere Ursache von Meldungen ist der Einsatz von mobilen Geräten wie Laptops und Smartphones mit Zugang zu Regierungsnetzen, die verloren gehen oder gestohlen werden. Konkrete Angriffe auf das Regierungsnetz mithilfe verlorener oder gestohlener Mobilgeräte sind jedoch bisher nicht zu verzeichnen.

3.2 Vorfälle bei Privatanwendern

3.2.1 Millionenfacher Identitätsdiebstahl in Deutschland

Sachverhalt

Im Frühjahr 2014 wurden zwei Identitätsdiebstähle publik, bei denen Angreifer Zugriff auf Benutzernamen und Passwörter von 16 bzw. 18 Millionen Internetnutzern erlangen konnten.

Methode

Die Kriminellen erlangten den Zugriff auf die Daten über mit Schadsoftware infizierte Systeme der Nutzer sowie mittels Angriffen auf Anbieter von Online-Diensten.

Schadenswirkung

Die Täter versuchten unter anderem, sich mit den E-Mail-Adressen und den zugehörigen Passwörtern in E-Mail-Accounts einzuloggen und diese für den Versand von Spam-Mails zu missbrauchen. Es ist davon auszugehen, dass es sich bei den gefundenen Adressen und Passwörtern sowohl um Zugangsdaten zu E-Mail-Konten als auch um Zugangsdaten zu anderen Online-Konten etwa bei Online-Shops, Internetforen oder Sozialen Netzwerken handelt.

Zielgruppen

Im Fokus der Angreifer standen Internetnutzer in Deutschland und anderen europäischen Ländern.

Technische Fähigkeiten

Angriffe auf Internetnutzer mittels E-Mails mit Schadsoftware, Social Engineering oder Drive-by-Exploits gehören heute zum Alltag. Die große Anzahl der Anfang des Jahres aufgefundenen Nutzerdaten spricht jedoch für die Professionalität der Täter.

3.2.2 Schwachstellen in Routern für Heimnetzwerke

Sachverhalt

Anfang 2014 wurde eine Schwachstelle in Fritz!-Box-Routern des Herstellers AVM bekannt.

Methode

Angreifer nutzten eine ungepatchte Schwachstelle aus, um Zugriff auf das Gerät und auf sämtliche im Router gespeicherten Konfigurationsdaten zu erhalten.

Schadenswirkung

Mit dem Zugriff auf die Konfigurationsdaten konnten die Angreifer Manipulationen im System vornehmen. Zudem bestand die Möglichkeit, Zugangsdaten zu E-Mail-Konten oder anderen Online-Diensten auszulesen, sofern der Besitzer diese auf dem Router hinterlegt hatte. Darüber hinaus nutzten Angreifer die Schwachstelle, um zu Lasten der Opfer bzw. der Telefonanbieter kostenpflichtige Telefonate zu teuren Sonder-Nummern zu führen. Der Hersteller hat durch mehrere Informationsaufrufe die Nutzer auf die Notwendigkeit des Sicherheitsupdates hingewiesen.

Zielgruppen

Mehrere Millionen Geräte von Privatanwendern waren allein in Deutschland betroffen. Daneben waren auch KMUs und andere Unternehmen betroffen, die diese Geräte in ihren Betrieben einsetzen.

Technische Fähigkeiten

Sowohl technisch als auch organisatorisch gingen die Täter professionell vor, indem sie eine bis dahin unbekannte Sicherheitslücke im Betriebssystem der Router ausnutzten, um Informationen auszuspähen und einen finanziellen Schaden bei den Opfern zu verursachen.

3.2.3 Online-Banking-Trojaner: von Feodo zu Geodo

Sachverhalt

Die Online-Banking-Schadsoftware Geodo folgte im Mai 2014 auf den 2013 bekannt gewordenen Trojaner Feodo.

Methode

Die Angreifer verbreiten per E-Mail mittels täuschend echt aussehender Rechnungen bzw. Buchungsbestätigungen im Namen von Telekommunikationsdienstleistern und Banken ein Schadprogramm, das entweder als Datei angehängt oder verlinkt war. Die Links führten zu kompromittierten Webseiten, auf denen die Angreifer das Schadprogramm zum Download abgelegt hatten.

Schadenswirkung

Die über mehrere Wochen laufenden Angriffswellen waren – wie schon im Falle von Feodo – sehr erfolgreich und führten zu einer großen Zahl von Infektionen. Neben der Manipulation von Online-Banking-Vorgängen späht Geodo auf infizierten PCs Zugangsdaten für E-Mail-Konten aus und übermittelt diese an Kontrollserver der Angreifer. Diese Zugangsdaten werden anschließend für die weitere Verbreitung der Schadsoftware missbraucht.

Zielgruppen

Im Fokus der Angreifer standen insbesondere Internetnutzer und Bankkunden in Deutschland.

Technische Fähigkeiten

Das beim BSI angesiedelte Computer Emergency Response Team der Bundesverwaltung (CERT-Bund) übernahm die Rolle eines Bot und ließ sich über drei Wochen Pakete gestohlener Zugangsdaten von den Kontrollservern übermitteln. Insgesamt konnten so über 200.000 kompromittierte E-Mail-Konten identifiziert werden. CERT-Bund hat die jeweils zuständigen Netzbetreiber über die kompromittierten E-Mail-Konten informiert. Die Fähigkeiten der Schadsoftware sowie die direkte Weiterverwertung abgegriffener Zugriffsdaten für Spam sprechen für einen technisch wie organisatorisch aufwendigen Angriff auf deutsche Anwender.

3.2.4 iBanking: Schadsoftware für Smartphones

Sachverhalt

Seit Mitte 2013 wird in Untergrundforen Schadsoftware zur Überwachung und Manipulation von Android-Smartphones angeboten. Die Schadsoftware wurde unter anderem für Angriffe auf das Online-Banking mit mTANs verwendet.

Methode

Zunächst wird der PC des Opfers mit einem Schadprogramm infiziert. Bei der darauf folgenden Anmeldung zum Online-Banking manipuliert das Schadprogramm die Webseite der Bank und fordert Informationen zum Mobiltelefon des Opfers an. Das Opfer erhält daraufhin eine SMS mit einem Link zu einer mit iBanking infizierten App und wird mittels Social Engineering dazu gebracht, diese App auf seinem Smartphone zu installieren. Der Angriff auf das Online-Banking erfolgt durch das Zusammenspiel der Schadprogramme auf dem PC und dem Smartphone. Das Schadprogramm auf dem PC startet eine eigene Geldüberweisung. Die mTAN, die die Bank an das Mobiltelefon des Kunden schickt, wird dort von iBanking abgefangen und an den infizierten PC übermittelt. Mit der abgefangenen mTAN schließt das Schadprogramm auf dem PC die eigene Überweisung ab.

Schadenswirkung

Die Angreifer waren in der Lage, das Online-Banking einiger internationaler Banken zu kompromittieren. Die Schadsoftware kann relativ einfach auch für Angriffe auf weitere Internetdienste angepasst werden. So wurden bereits Varianten von iBanking entdeckt, die Angriffe auf die Zwei-Faktor-Authentifizierung (Benutzername/Passwort + SMS-Code) bei Facebook und Gmail ermöglichen.

Zielgruppen

Mit der Schadsoftware werden Bankkunden angegriffen, die das Online-Banking mit mTANs verwenden.

Technische Fähigkeiten

Die Schadsoftware bietet den Angreifern umfassende Möglichkeiten zur Kontrolle eines Smartphones: Überwachung des SMS-Verkehrs, Aufzeichnung von Telefonanrufen, akustische Raumüberwachung, Zugriff auf diverse Daten auf dem Smartphone etc. Alle gesammelten Informationen können auf einen vom Angreifer kontrollierten Server übermittelt werden. Im Paket mit iBanking bieten die Entwickler auch Serversoftware an, mit der die infizierten Geräte verwaltet werden können. Die Funktionalität der Schadsoftware zeugt vom hohen technischen Know-how der Entwickler, die ihre Software unter verschiedenen Lizenzmodellen an alle Interessenten verkaufen.

3.3 Vorfälle in der Wirtschaft

Anders als in der Bundesverwaltung gibt es bislang keine Verpflichtung für Unternehmen, gravierende IT-Sicherheitsvorfälle an das BSI zu melden. Im Rahmen des UP KRITIS besteht für die teilnehmenden Betreiber Kritischer Infrastrukturen seit vielen Jahren die Möglichkeit, sich zu Vorfällen auszutauschen. Das BSI bietet zudem mit der Allianz für Cyber-Sicherheit eine Meldestelle an, über die auch anonym Vorfälle gemeldet werden können, die eine Relevanz für andere Stellen haben könnten oder zu denen eine Bewertung oder Hilfestellung gewünscht ist. Ziel der Meldestelle ist es, Erkenntnisse über neuartige Angriffstechniken oder kritische Vorfälle mit übergreifenden Auswirkungen zu gewinnen. Das BSI analysiert die Meldungen und stellt die Auswertungen aufbereitet und anonymisiert einem größeren Adressatenkreis zur Verfügung. Mit dieser Vorgehensweise sollen anderen Unternehmen frühzeitig Erkenntnisse über neue Angriffe und mögliche Präventionsmaßnahmen zur Verfügung gestellt werden. Bislang wenden sich überwiegend kleinere und mittlere Unternehmen an die Meldestelle, die Opfer von DDoS-Angriffen oder Schadprogramminfektionen geworden sind.

3.3.1 APT-Angriff auf Industrieanlagen in Deutschland

Sachverhalt

Gezielter Angriff auf ein Stahlwerk in Deutschland.

Methode

Mittels Spear-Phishing und ausgefeiltem Social Engineering erlangten Angreifer initialen Zugriff auf das Büronetz des Stahlwerks. Von dort aus arbeiteten sie sich sukzessive bis in die Produktionsnetze vor.

Schadenswirkung

Es häuften sich Ausfälle einzelner Steuerungskomponenten oder ganzer Anlagen. Die Ausfälle führten dazu, dass ein Hochofen nicht geregelt heruntergefahren werden konnte und sich in einem undefinierten Zustand befand. Die Folge waren massive Beschädigungen der Anlage.

Zielgruppen

Betreiber von Industrieanlagen.

Technische Fähigkeiten

Die technischen Fähigkeiten der Angreifer sind als sehr fortgeschritten zu bewerten. Die Kompromittierung erstreckte sich auf eine Vielzahl unterschiedlicher interner Systeme bis hin zu industriellen Komponenten. Das Know-how der Angreifer

war nicht nur im Bereich der klassischen IT-Sicherheit sehr ausgeprägt, sondern erstreckte sich auch auf detailliertes Fachwissen zu den eingesetzten Industriesteuerungen und Produktionsprozessen.

3.3.2 Heartbleed – kritische Schwachstelle in weit verbreiteter Softwarebibliothek

Sachverhalt

Über die als Heartbleed bezeichnete Schwachstelle, die im April 2014 in der Softwarebibliothek OpenSSL entdeckt wurde, können unerlaubt Speicherinhalte ausgelesen werden.

Methode

Zum Ausnutzen der Schwachstelle reicht es aus, spezielle Anfragen an ein System zu senden, das die von der Schwachstelle betroffene Funktion von OpenSSL verwendet.

Schadenswirkung

Das Secure-Sockets-Layer-Protokoll (SSL-Protokoll) oder Transport Layer Security (TLS) nutzt nahezu jeder Internetnutzer, meistens jedoch, ohne es zu wissen. Die an vielen unterschiedlichen Stellen eingesetzte Technik hat große Bedeutung für die verschlüsselte Kommunikation im Internet und wird zum Beispiel auf fast allen Webseiten eingesetzt, um deren Authentizität zu überprüfen und die Kommunikation zwischen Nutzer und Webseite zu verschlüsseln. Häufig kommt dafür die freie Softwarebibliothek OpenSSL zum Einsatz. Durch die Schwachstelle Heartbleed in der Softwarebibliothek OpenSSL können unerlaubt Speicherinhalte ausgelesen werden. Dabei kann es sich um Benutzernamen und Passwörter handeln, die von Besuchern auf der Webseite eingegeben wurden. In seltenen Fällen können aber auch geheime Schlüssel ausgelesen werden. Damit könnte sich ein Angreifer als vermeintlicher Diensteanbieter ausgeben und den eigentlich verschlüsselten Datenverkehr der Nutzer mitlesen.

Zielgruppen

Von der Sicherheitslücke waren alle Produkte und Dienste betroffen, die die verwundbare Funktion der Softwarebibliothek OpenSSL verwenden. Neben großen Online-Diensten, Sozialen Netzwerken oder Webseiten von Banken waren auch Server der Bundesverwaltung von der Schwachstelle betroffen. Aufgrund der Reichweite der Schwachstelle ist davon auszugehen, dass es trotz vorhandener Patches auch weiterhin Systeme in Deutschland gibt, die von Heartbleed beeinträchtigt werden können.

3.3.3 Dragonfly – gezielte Angriffe auf Produktionsnetze

Sachverhalt

Mit dem 2014 bekannt gewordenen Schadprogramm Havex griff die sogenannte Dragonfly-Gruppe (auch geläufig unter dem Namen Energetic Bear) mehrere Dutzend deutsche Unternehmen an.

Methode

Im Rahmen der Angriffskampagne kam ein neuer Angriffsweg zum Einsatz: Im ersten Schritt griffen die Täter die Hersteller von Software für Industriesteuerungssysteme an. Den entsprechenden Installationsdateien auf den Downloadservern der Anbieter wurde das Schadprogramm Havex angehängt, sodass die Kunden bei der Installation der legitimen Software zugleich auch die Schadsoftware auf ihr System brachten. In einigen Fällen wurde von dieser dann ein Modul nachgeladen, das gezielt Informationen über die im Produktionsnetz verwendeten Geräte und Systeme sammelte und an die Täter weiterleitete.

Schadenswirkung

Mittels Havex wurde gezielt Schadsoftware im Bereich industrieller Steuerungssysteme eingesetzt, um Informationen zu sammeln. Es ist davon auszugehen, dass die Täter diese Informationen in einem nächsten Schritt für weitere Angriffe verwenden. In Zusammenarbeit mit dem Bundeskriminalamt informierte das BSI mehrere Dutzend Firmen in Deutschland, die Opfer der Dragonfly-Kampagne wurden.

Zielgruppen

Produktionsanlagen und Produktionsnetze.

Technische Fähigkeiten

Die im Rahmen der Angriffskampagne Dragonfly sichtbar gewordenen Fähigkeiten, wie bspw. die gezielte Kompromittierung von Downloadservern, verdeutlichen das hohe technische Niveau der Angreifer und belegen, dass Angriffe auf Industriesteuerungssysteme in Deutschland Realität sind.

3.3.4 Operation Windigo – Linux-Schadprogramm Ebury sammelt SSH-Zugangsdaten

Sachverhalt

Ebury ist ein Schadprogramm mit Backdoor-Funktionalität – ein sogenanntes Rootkit – für Linux und Unix-ähnliche Betriebssysteme, das Secure-Shell(SSH)-Zugangsdaten ausspäht.

Methode

Das Schadprogramm wird von Angreifern auf kompromittierten Servern entweder durch den Austausch von SSH-Programmdateien oder einer von diesen Programmen gemeinsam genutzten Bibliothek installiert. Auf infizierten Systemen stiehlt Ebury Zugangsdaten (Benutzernamen und Passwörter) von ein- und ausgehenden SSH-Verbindungen und sendet diese über das Internet an die Angreifer. Zusätzlich werden auf den kompromittierten Systemen für ausgehende SSH-Verbindungen verwendete private SSH-Schlüssel gestohlen.

Schadenswirkung

Über die Backdoor haben die Täter jederzeit die vollständige Kontrolle über das infizierte System. Die mit Ebury infizierten Server werden von den Tätern im Rahmen der Operation Windigo für verschiedene kriminelle Aktivitäten missbraucht. So wurden Webserver derart manipuliert, dass sie Besucher der dort gehosteten Webseiten auf andere Server umleiten. Dabei handelt es sich entweder um Dating-Portale, Webseiten mit pornografischen Inhalten oder um Server, die Drive-by-Exploits ausliefern und dadurch die Rechner der Webseiten-Besucher mit Schadsoftware infizieren. Bei der Analyse konnten mehrere hunderttausend derartiger Umleitungen täglich beobachtet werden. Auf weiteren Systemen installierten die Täter unter Ausnutzung der mittels Ebury ausgespähten Zugangsdaten Schadprogramme zum Versand von Spam-Mails. Im Beobachtungszeitraum konnte hierüber der Versand von durchschnittlich 35 Millionen Spam-Mails täglich beobachtet werden.

Zielgruppen

Serverbetreiber (primär) sowie Internetnutzer (sekundär).

Technische Fähigkeiten

Ebury ist von hoher technischer Qualität und die aus den kompromittierten Servern aufgebaute Infrastruktur ist professionell organisiert. Die Täter erzielen durch die Verbreitung von Schadsoftware mittels Drive-by-Exploits, Umleitungen von Webseiten sowie durch den Spam-Versand hohe finanzielle Gewinne. CERT-Bund beteiligte sich an der „Ebury Working Group“, einem internationalen Zusammenschluss von Sicherheitsanalysten, die

seit Februar 2013 weltweit rund 30.000 mit Ebury infizierte Server identifiziert hat. Etwa zehn Prozent dieser Server stehen in Deutschland. CERT-Bund benachrichtigt regelmäßig deutsche Hosting-Provider sowie nationale CERTs in über 60 Ländern über erkannte Ebury-Infektionen.

3.3.5 Großbritannien: Bankrott infolge von Cyber-Erpressung und -Sabotage

Sachverhalt

Im Juni 2014 wurde die Austausch- und Entwicklungsplattform für Softwareentwickler der Firma Code Spaces zum Ziel einer Erpressung, die von einem mehr als 48 Stunden andauernden DDoS-Angriff begleitet wurde.

Methode

Die Täter erlangten illegal Zugriff auf einen Administratorenzugang des durch das Unternehmen bei Amazon Web Services angemieteten Cloud-Speicherplatzes und platzierten dort mehrere Nachrichten mit ihren Geldforderungen. Auf die absehbare, aber wirkungslose Änderung der Zugangsdaten durch Code Spaces hatten sie sich offenbar bereits vorab vorbereitet.

Schadenswirkung

Nachdem das Unternehmen nicht auf die Zahlungsforderungen einging, begannen die Täter damit, wahllos Daten zu löschen. Dabei gingen nahezu alle Daten, Backups und Maschineneinstellungen verloren. Das bereits sieben Jahre am Markt tätige Unternehmen war letztendlich gezwungen, seinen Betrieb einzustellen. Eine Reaktivierung ist den Verantwortlichen zufolge nicht geplant, da die finanziellen Belastungen durch Wiederherstellungsmaßnahmen und Entschädigungsforderungen der Kunden nicht zu bewältigen seien.

Zielgruppen

Der Angriff illustriert das grundsätzliche Risiko eines unternehmerischen Kollapses durch Erpressung und Sabotage im Cyber-Raum sowie durch das Outsourcing geschäftskritischer Dienstleistungen.

3.3.6 ShellShock – Schwachstelle im Kommandozeileninterpreter Bash

Sachverhalt

Im September 2014 wurde unter dem Namen ShellShock eine Schwachstelle im Kommandozeileninterpreter Bash bekannt. Bash erlaubt nicht nur die Weitergabe von Umgebungsvariablen an eine Shell, sondern auch von Funktionen. Dabei wird der Funktionsname als Umgebungsvariable, gefolgt von der Funktionsdefinition, an die Shell übergeben. Die Schwachstelle ermöglicht es, dass ein angehängter Programmcode in Funktionsdefinitionen ausgeführt wird.

Methode

Bash ist eine Standardkomponente und entsprechend weit verbreitet. Sie wird unter anderem für Systemdienste und Fernzugriffe sowie auf Web- und Mailservern und bestimmten Smartphones verwendet. Dementsprechend vielfältig sind die Szenarien, in denen die Schwachstelle ausgenutzt werden kann, um unerlaubt Programmcode auf betroffenen IT-Systemen auszuführen. Sind über das Internet verbundene Dienste von ShellShock betroffen, kann die Schwachstelle auch aus der Ferne ausgenutzt werden.

Schadenswirkung

Durch die unerlaubte Ausführung von Programmcode, unter Umständen mit Administratorenrechten, können Angreifer vertrauliche Informationen auslesen, Manipulationen am IT-System vornehmen oder das IT-System stören. Es wurden Schadprogramme beobachtet, die die Schwachstelle ausgenutzt haben, um IT-Systeme außer Funktion zu setzen. ShellShock hat auf der Skala des anerkannten Schwachstellenbewertungssystems CVSS die höchste Bewertung 10 erhalten.

Zielgruppen

Bash ist die Standard-Shell der meisten Linux-Distributionen und ist auch auf vielen anderen Systemen mit installiert. Betroffen sind auch Apples Betriebssystem OS X sowie bestimmte Industriesteuerungssysteme. Es ist davon auszugehen, dass sich zum Zeitpunkt des Bekanntwerdens in praktisch jeder Institution verwundbare Systeme befanden.

3.4 Vorfälle im Bereich Kritischer Infrastrukturen (KRITIS)

3.4.1 Social Engineering bei Großkonzernen

Sachverhalt

Im Mai 2014 wurden hochrangige Vertreter mehrerer international tätiger Großunternehmen mit besonders ausgefeilten Phishing-Mails adressiert.

Methode

Mit fingierten E-Mails wurden die Mitarbeiter darüber informiert, dass infolge eines Updates im IT-System zur Personalverwaltung ein Verdacht auf Inkonsistenzen in einzelnen Datensätzen bestehe. Unter diesem Vorwand wurden die Adressaten aufgefordert, die Kopie eines amtlichen Lichtbildausweises und die Bankverbindung ihres Gehaltskontos zu übermitteln. Die E-Mails in nahezu perfekter deutscher bzw. englischer Sprache enthielten die Legende einer vollständigen Mailhistorie samt E-Mail-Headern mit authentischen Firmen-E-Mail-Adressen, um den Vorgang augenscheinlich zu legitimieren. Bemerkenswert war, dass die in der gefälschten Historie genannten Mitarbeiter tatsächlich in den jeweiligen Personalabteilungen tätig sind.

Schadenswirkung

Einzelne Adressaten hielten die E-Mail für authentisch und übermittelten die angeforderten Dokumentenkopien bzw. Kontodaten an den Absender. Daraufhin wurden von den Angreifern postalisch mit gefälschten Unterschriften die Bankkonten der Betroffenen aufgelöst oder neue EC-Karten samt PIN an eine neue Adresse in China angefordert.

Zielgruppen

Hochrangige Mitarbeiter deutscher Großkonzerne.

Technische Fähigkeiten

Der Aufwand für Planung und Recherche eines derartigen Angriffs ist als sehr hoch einzuschätzen, sodass von äußerst versierten Angreifern ausgegangen werden muss. Auffällig ist der nahezu perfekte Gebrauch der deutschen Sprache, wodurch sich dieser Angriff von vielen anderen Attacken dieser Art unterscheidet.

3.4.2 Österreich: Fehlfunktion in der Steuerung von Energienetzen

Sachverhalt

2013 wurden in verschiedenen österreichischen Leittechniknetzwerken für die Steuerung von Energienetzen Anomalien im Datenstrom festgestellt. Diese verursachten bei mehreren Verteilnetz- und Kraftwerksbetreibern Einschränkungen sowie vereinzelte Ausfälle in der Datenübertragung.

Methode

Die Fehlfunktion wurde vermutlich durch einen Steuerungsbefehl im Rahmen einer Inbetriebnahme im Netzwerk eines Gasnetzbetreibers im Süden Deutschlands ausgelöst und erreichte auch das österreichische Energienetz. Es erfolgte eine Weiterleitung an unterschiedliche Betreiber. Aufgrund der nicht spezifizierten Verarbeitung dieser Nachricht in einzelnen Komponenten des Netzwerks wurde der Befehl in einer Endlosschleife versendet. Diese löste erhebliche Störungen der Leittechnik für die Netzsteuerung aus.

Schadenswirkung

Die Netzstabilität konnte während des Vorfalls nur unter hohem Aufwand sichergestellt werden. Während der Störung wurden erhebliche Datenmengen erzeugt, die zu Logdaten-Überläufen führten. Die Ursache des Vorfalls ließ sich deshalb nicht abschließend analysieren.

Zielgruppe

Betreiber von Energienetzen.

3.4.3 USA: IT-Manipulation im Hochfrequenzhandel eines US-Hedgefonds

Sachverhalt

Hochfrequenzhandel ist der An- und Verkauf großer Mengen an Wertpapieren in extrem kurzen Zeitabständen. Das System eines US-Hedgefonds, mit dem der Hochfrequenzhandel („high-frequency trading“, HFT) durchgeführt wird, wurde durch einen Cyber-Angriff manipuliert.

Methode

Ende 2013 drangen kriminelle Hacker in das Rechnernetzwerk eines US-amerikanischen Hedgefonds ein. Dadurch konnten sie die von dem Fondsbetreiber legitim eingespeisten Handelsaufträge abfangen, mitlesen und deren Weiterleitung um Millisekunden verzögern. Dies blieb über mehrere Monate unentdeckt.

Schadenswirkung

Unter Verwertung der ausgespähten Orderdaten übermittelten die Täter in diesem kurzen Zeitfenster vor der Weiterleitung ihrerseits Handelsaufträge zulasten des Hedgefonds-Betreibers.

Der Vorfall ist in zweierlei Hinsicht bemerkenswert: Zum einen illustriert er – nach dem „Flash Crash“ im Jahr 2010 – zum wiederholten Mal die starke Verwundbarkeit des Börsenbetriebs gegen Cyber-Angriffe. Zum anderen ist neu, dass die Täter die ausgespähten Daten selbst für eigenen Handel nutzten. In der Vergangenheit hat es bereits marktverzerrende Effekte und teilweise Ausfälle von HFT-Handelsplattformen durch fehlerhafte HFT-Software gegeben.

Zielgruppen

Einrichtungen des Finanzsektors.

Technische Fähigkeiten

Für Angriffe dieser Art gehören ausgewiesene technische Fähigkeiten und eine passende Infrastruktur zur Grundvoraussetzung. Hinzu kommt, dass detailliertes Domänenwissen im Hochfrequenzhandel notwendig ist, um den zeitlichen Vorsprung im Bereich von Millisekunden ausnutzen und zu Geld machen zu können.

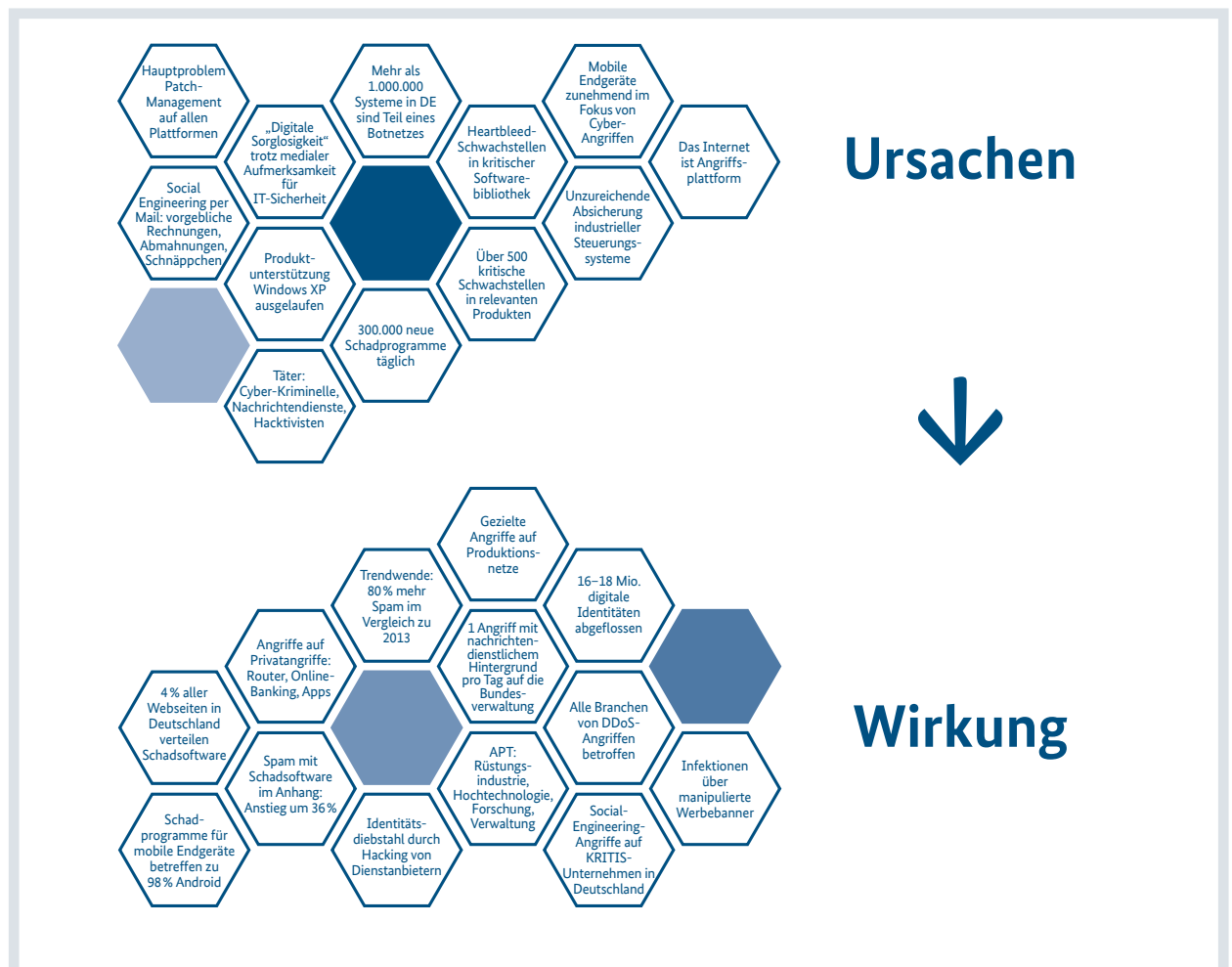


Abbildung 9: Überblick: Ursachen und Wirkung der Gefährdungslage und der Vorfälle

4 Lösungsansätze

4 Lösungsansätze

Lösungsansätze zur Verbesserung der Risikosituation im Cyber-Raum müssen auf die Entwicklung zielgruppengerechter Maßnahmen abzielen und insbesondere die Wirtschaft sowie die Bürgerinnen und Bürger beim Selbstschutz unterstützen. Wesentliches Merkmal der Maßnahmen muss deren Skalierbarkeit sein, um orientiert am Schutzbedarf des Einzelnen bzw. der Einrichtung die angemessene Maßnahme auswählen zu können. Aus der dargestellten Gefährdungslage sowie den genannten Herausforderungen der aktuellen IT-Landschaft lassen sich nachfolgende Maßnahmenbereiche ableiten.

4.1 Kompetenz und Vertrauenswürdigkeit im Bereich IT-Sicherheit fördern

Grundvoraussetzung für die Gewährleistung von Informationssicherheit sind effektive und vertrauenswürdige Sicherheitsmechanismen auf technischer Ebene. Denn Manipulationen an IT-Komponenten können auch mit einem hohen Prüfaufwand nicht vollständig ausgeschlossen werden. Somit wird die Förderung des Angebots an vertrauenswürdiger Informationstechnik zu einer zentralen Säule für die Gewährleistung eines hohen Niveaus der IT-Sicherheit in Deutschland. Dies ist auch mit Blick auf die jüngste Diskussion über die Aktivitäten ausländischer Nachrichtendienste im Cyber-Raum von Bedeutung.

Grundsätzlich sollte sich das gemeinsame Handeln von Staat, Wirtschaft und Forschung dabei an folgenden strategischen Zielen ausrichten:

- Schutz von Grundwerten in der digitalen Welt durch die Sicherung der technologischen Handlungsfähigkeit und die Förderung vertrauenswürdiger Informationstechnik.
- Schaffung von Rahmenbedingungen und Anreizen, um ausländische Marktführer dazu zu veranlassen, ihre Produkte auf technischer Ebene durch Vertrauensanker (beispielsweise nationale Kryptokomponenten) an deutsche Vertraulichkeitsansprüche anzupassen – insbesondere bei höheren Sicherheitsanforderungen.
- Befähigung der deutschen Wirtschaft, industrielle Kernkompetenzen mit dem in Deutschland vorhandenen Know-how im Bereich der Informationssicherheit zu verbinden, um notwendige IT-Sicherheitsstandards in zentralen Wirtschaftsbereichen durchsetzen zu können.

Zu den wesentlichen Erfolgsvoraussetzungen zählt die Entwicklung nachhaltiger Geschäftsmodelle, um den langfristigen Erfolg dieser Angebote am Markt zu sichern. IT-Sicherheit kann hierbei ein wichtiger Faktor zur Angebotsdifferenzierung gegenüber Mitbewerbern für eine starke Wettbewerbsposition in wichtigen Zukunftsmärkten sein (vertrauenswürdige Lösungen „Made in Germany“). Beispiel einer solchen vom BSI konzipierten und geförderten Technologie ist die SINA-Produktfamilie, bei der IT-gestützte „Sichere Arbeitsplätze“ bereitgestellt werden, die es ermöglichen, trotz Vertrauensdefizit die Anwendungsproduktlinien der Marktführer risikofrei nutzen zu können.

Deutsche E-Mail-Anbieter bewerben in einer gemeinsamen Aktion ein vertrauenswürdiges Dienstleistungsangebot „eMail Made in Germany“. Derartige Angebote können durch die Standardisierung entsprechender Kriterien für Sicherheit und Vertrauenswürdigkeit sowie ggf. durch die Erteilung eines entsprechenden Zertifikates unterstützt werden.

In der schnelllebigen IT-Welt muss bei allen tagesaktuellen Aktivitäten auch stets der Blick nach vorn gerichtet werden. So steigt etwa der Integrationsbedarf von höherwertigen Sicherheitsmechanismen in Smartphones mit der Perspektive, dass Smartphones künftig für Bezahl- und Geldtransferzwecke intensiver genutzt werden. Grundvoraussetzung für die Gewährleistung von Informationssicherheit sind effektive und vertrauenswürdige Sicherheitsmechanismen auf technischer Ebene. Auch Bereiche, die von diesem Lagebild noch nicht erfasst worden sind, wie E-Health, Smart City und Automotive mit partiellen Bezügen zu Safety (Sicherheit von Leib und Leben), können künftig höhere Sicherheitsanforderungen zur Folge haben. Als perspektivische Herausforderungen sind zudem die Bereiche Krypto- und Cyber-Technologien, Cloud-Lösungen, Sicherheitstechnologien zum Schutz von Industriesteueranlagen und Entwicklungen für intelligente Netze (SDN) zu sehen.

4.2 Engagement für Standardisierung und Zertifizierung

Mit der Standardisierung und Zertifizierung stehen effektive Instrumente zur Verfügung, um die Transparenz im Bereich der Informations-

sicherheit zu erhöhen, die Vertrauenswürdigkeit von Produkten und Dienstleistungen zu bewerten und ein hohes Niveau der Informationssicherheit am Markt durchsetzen zu können. Deutschland verfügt im Bereich der IT-Sicherheit über ein leistungsfähiges Zertifizierungsschema und international renommierte Prüfstellen.

Nichtsdestotrotz sind verstärkte Anstrengungen erforderlich, um diese Spitzenposition zu sichern und neuen technologischen Herausforderungen gerecht zu werden. Zudem bestehen Defizite im Bereich der Vertretung Deutschlands in internationalen Standardisierungsgremien. Führende Unternehmen aus dem Bereich der Informations- und Kommunikationstechnik zielen häufig darauf ab, proprietäre Standards in internationalen Standardisierungsgremien durchzusetzen, um sich auf diese Weise Wettbewerbsvorteile zu sichern. Dadurch werden Sicherheitsstandards am Markt etabliert, die häufig deutlich unterhalb eines aus informationstechnischer Sicht empfehlenswerten Niveaus angesiedelt sind.

Es bedarf deswegen einer verstärkten Koordination des Engagements von Wirtschaft und Staat im Bereich der IT-Standardisierung mit besonderem Bezug zur IT-Sicherheit, die insbesondere auch Technologieoffenheit und den Ansatz offener Standards vertritt.

Der Bund ist bereits jetzt aktiv mit Vorgaben zu IT-Sicherheitsstandards, beispielsweise in Form von Technischen Richtlinien und BSI-Standards, in sicherheitskritischen Bereichen, um die Entwicklung nationaler Best-Practice-Lösungen zu fördern. So kooperiert das BSI etwa bei der Umsetzung des Energiewirtschaftsgesetzes mit den Messsystemherstellern der Energiebranche bei der Entwicklung von Schutzprofilen und einer Technischen Richtlinie für die intelligenten Messsysteme des künftigen Smart Grid. Diese technischen Standards werden gemeinsam mit der gesamten Branche entwickelt und finden in den Anforderungen des VDE/FNN für das Messsystem 2020 ihre Entsprechung.

Vorliegende Marktanalysen prognostizieren, dass der Bedarf an Dienstleistungen zur Abwehr von Cyber-Angriffen weiter an Bedeutung gewinnen wird. Mit der perspektivischen Etablierung von nationalen Cyber-Sicherheitsdienstleistern bietet sich als Nachweis für Kompetenz und Vertrauenswürdigkeit die Zertifizierung entsprechender Unternehmen an. In Teilgebieten wie IS-Revision, Beratung und Penetrationstests hat das BSI bereits Dienstleister zertifiziert.

Im Industriesektor sei auf den Bedarf einer verstärkten Mitwirkung an dem im Industrieumfeld

wichtigen Standard OPC UA (zentrales Protokoll im Rahmen von Industrie 4.0) verwiesen – einem der Zukunftsfelder für die deutsche Industrie, um sich als Nutzer und Anbieter zu positionieren. Das BSI arbeitet gemeinsam mit einem führenden Branchenverband an Standards für eine sichere Datenübertragung.

4.3 IT-Sicherheit in der Gesellschaft und breitflächige Anwendung sicherer Technologien fördern

Voraussetzung für den Einsatz von Sicherheitstechnik ist die Sensibilität der Nutzer für die Gefährdungen der IT. Jeder Nutzer trägt die Eigenverantwortung für seine IT und muss daher auch selbst für die Sicherheitsmaßnahmen Sorge tragen. Nur durch eigeninitiiertes Handeln kann er sich gegen bestimmte in Kapitel 2 beschriebene Gefährdungen schützen. Das BSI hält als nationale IT-Sicherheitsbehörde für die verschiedenen Zielgruppen unterschiedliche Angebote zur Unterstützung bereit.²⁰

Darüber hinaus ist die Förderung des Einsatzes sicherer und vertrauenswürdiger Technologien in der Breite eine weitere wesentliche Voraussetzung für die Erhöhung der IT-Sicherheit in Deutschland. Aus informationstechnischer Sicht ist insbesondere die Entwicklung, Bereitstellung und durchgängige Anwendung vertrauenswürdiger Krypto- und Cyber-Technologien für alle Zielgruppen von entscheidender Bedeutung, um die aus der kritischen Gefährdungslage resultierenden Risiken zu minimieren.

Wesentlich ist dabei die Bereitstellung skalierbarer Cyber-Sicherheitsangebote, die ein an die spezifischen Bedürfnisse der unterschiedlichen Zielgruppen angepasstes Schutzniveau ermöglichen. Da bereits mehr als 80 Prozent der Bedrohungen im Cyber-Raum durch die Umsetzung grundlegender Sicherheitsmaßnahmen abgewehrt werden können, ist es erforderlich, Basistechnologien für die Zielgruppe der Bürgerinnen und Bürger sowie für kleine und mittlere Unternehmen (KMU) zur Verfügung zu stellen. Diese werden so in die Lage versetzt, eigenverantwortlich einen Beitrag zu mehr Sicherheit im Cyber-Raum zu leisten. Notwendig ist in diesem Zusammenhang auch die Bereitstellung von Gesamtlösungen, die Clients in Kombination mit Krypto- und Cyber-Sicherheitsmechanismen gegen Bedrohungen auf unterschiedlichen Ebenen schützen.

Der Staat hat durch seine Gestaltungsmöglichkeiten beispielsweise mit De-Mail erstmals eine übergreifende PKI-Infrastruktur in Deutschland

geschaffen. Die Lösung wird künftig neben der Transportverschlüsselung auch Ende-zu-Ende-Verschlüsselung unterstützen. Zurzeit werden über 90 Prozent der E-Mails unverschlüsselt übertragen. Zudem bietet De-Mail mit der Zwei-Faktor-Authentifizierung Sicherheitsmechanismen gegen Identitätsdiebstahl, dessen Angriffspunkt oftmals das gängige softwaregestützte Passwortverfahren ist.

Eine weitere mittelbare Förderung der IT-Sicherheit in der Gesellschaft stellt die permanente Sicherheitsanalyse der universell eingesetzten Open-Source-IT-Sicherheits- und -Kryptobibliotheken sowie deren begleitende sicherheitstechnische Fortentwicklung und Pflege dar. Schwachstellen wie Heartbleed mit immenser Breitenwirkung könnten so weitestgehend vermieden und eine nachhaltige Verbesserung der Sicherheitseigenschaften dieser Softwarebibliotheken könnte erreicht werden.

Die Wirtschaft ist in diesem Kontext als Anbieter von IT-Sicherheitslösungen gefordert. Provider könnten ihren Kunden flächendeckend einfach zu bedienende IT-Sicherheitslösungen zur Verfügung stellen. Wesentliches Erfolgskriterium wird hier eine nahezu vollständige Automation der Einrichtung der Sicherheitsfunktionalität sein. Auch Online-Anbieter könnten Bürgerinnen und Bürgern verstärkt schützen, beispielsweise durch die Einführung von Verfahren mit Mehrfaktor-Authentifizierung zum Schutz vor Identitätsdiebstahl.

Zugleich ist die Wirtschaft auch als Betroffene von Cyber-Angriffen gerade im Kontext von Cyber-Spionage zu sehen. So sind insbesondere Mechanismen zu entwickeln und durchgehend zur Anwendung zu bringen, die einen adäquaten Schutz gegen besonders hochwertige Angriffsformen wie etwa Advanced Persistent Threats (APT) bieten. Hierfür ist eine enge Kooperation zwischen Staat, Wirtschaft und auch Wissenschaft gefordert, um Angriffe und Angriffsformen möglichst frühzeitig zu erkennen, ein gemeinsames Lagebild zu erstellen und dieses Wissen inklusive Abwehrmechanismen zu teilen, wie dies bereits im CERT-Verbund erfolgt. Zentrale Kooperationsplattform für Staat und Wirtschaft ist zudem die Allianz für Cyber-Sicherheit, an der aktuell rund 1.000 Unternehmen und Institutionen partizipieren und in der bereits 180 konkrete Empfehlungen ausgetauscht wurden. Der Ausbau solcher freiwilligen Modelle ist wesentlich, um sich in Anbetracht der dynamischen Technologie- und Lageentwicklung schnell und pragmatisch über Sicherheitslösungen und Abwehrmaßnahmen austauschen zu können.

Die vorliegenden Erkenntnisse zu ICS-Angriffen – Stuxnet gilt hier als Ausgangspunkt – rücken die

Sicherheit von ICS-Systemen in den Fokus und werden perspektivisch noch mehr Aufmerksamkeit binden. Um der Bedrohung gerecht zu werden, sollten insbesondere folgende Maßnahmen adressiert werden:

- Verstärkte Berücksichtigung von ICS-Security durch Computer Emergency Response Teams (CERTs) zum Schutz von Prozesssteuersystemen.
- Entwicklung von speziell auf Prozesssteuersysteme zugeschnittenen Sicherheitsprofilen auf System- und Produktebene sowie Entwicklung technologiespezifischer Mindeststandards.
- Stärkere Analyse von Angriffen auf Clouds sowie Entwicklung von Sicherheitsstandards und -maßnahmen.

4.4 Schutz Kritischer Infrastrukturen gewährleisten

Betreiber Kritischer Infrastrukturen sind wegen der möglichen weitreichenden gesellschaftlichen Folgen eines Ausfalls oder einer Beeinträchtigung der Versorgung und folglich ihrer besonderen Verantwortung für das Gemeinwohl in der Pflicht, einen Mindeststandard an IT-Sicherheit einzuhalten.

Die Bundesregierung pflegt entsprechend eine besonders enge Partnerschaft mit den Betreibern. So hat sich mit dem UP KRITIS seit 2007 zwischen Staat und KRITIS-Wirtschaft eine vertrauensvolle Kooperation etabliert.

Auch aufgrund der Entwicklung der Gefährdungslage seit 2011 ist eine weitere Vertiefung der Zusammenarbeit zwischen Staat und KRITIS-Betreibern notwendig. Der UP KRITIS wurde inhaltlich und strukturell fortgeschrieben und erlaubt nunmehr eine wesentlich tiefere Durchdringung der Branchen der Kritischen Infrastrukturen. Der vom Bundesministerium des Innern vorgelegte Entwurf eines IT-Sicherheitsgesetzes sieht unter anderem Mindeststandards und Meldepflichten für Betreiber Kritischer Infrastrukturen vor. Die eingehenden Meldungen sollen in ein Lagebild einfließen, das den Unternehmen zur Verfügung gestellt wird. Gleichzeitig kann auf Grundlage der gemeldeten Vorfälle die Unterstützung und Beratung der Wirtschaftsunternehmen durch das BSI gestärkt und optimiert werden. Bei IT-Sicherheitsvorfällen kann das BSI somit eine effektivere Unterstützung der KRITIS-Betreiber anbieten.

5 Glossar und Abkürzungsverzeichnis

Advanced Persistent Threats

Bei Advanced Persistent Threats (APT) handelt es sich um zielgerichtete Cyber-Angriffe auf ausgewählte Institutionen und Einrichtungen, bei denen sich ein Angreifer persistenten (dauerhaften) Zugriff zu einem Opfernnetzwerk verschafft und diesen in der Folge auf weitere Systeme ausweitet. Die Angriffe zeichnen sich durch einen sehr hohen Ressourceneinsatz und erhebliche technische Fähigkeiten aufseiten der Angreifer aus und sind in der Regel schwierig zu detektieren.

Adware

Als Adware werden Programme bezeichnet, die sich über Werbung finanzieren. Auch Schadprogramme, die Werbezwecken dienen, werden als Adware bezeichnet. Beim Herunterladen von Adware werden im Regelfall auch Programme installiert, die Spionagefunktionen ausüben. Darauf wird zumeist in den Lizenz- oder Nutzungsbedingungen hingewiesen.

Angriffsvektor

Als Angriffsvektor wird die Kombination von Angriffsweg und -technik bezeichnet, mit der sich ein Angreifer Zugang zu IT-Systemen verschafft.

Applikation/App

Eine Applikation, kurz App, ist eine Anwendungssoftware. Der Begriff wird oft im Zusammenhang mit Anwendungen für Smartphones oder Tablets verwendet.

Bot/Botnetz

Als Botnetz wird ein Verbund von Rechnern (Systemen) bezeichnet, die von einem fernsteuerbaren Schadprogramm (einem sogenannten Bot) befallen sind. Die betroffenen Systeme werden vom Botnetz-Betreiber mittels eines Command-and-Control-Servers (C&C-Server) kontrolliert und gesteuert.

Bürger-CERT

Das Bürger-CERT (siehe CERT/Computer Emergency Response Team) des BSI (www.buerger-cert.de) warnt Bürger und kleine Unternehmen schnell und kompetent vor Schadprogrammen sowie Sicherheitslücken in Computeranwendungen und informiert über Sicherheitsupdates.

Bring Your Own Device

Mit Bring Your Own Device (BYOD) wird die Nutzung privater Endgeräte für berufliche Zwecke sowie deren Einbindung in Unternehmensnetze bezeichnet.

CERT/Computer Emergency Response Team

Computer-Notfallteam, das aus IT-Spezialisten besteht. In vielen Unternehmen und Institutionen sind mittlerweile CERTs etabliert, die sich um die Abwehr von Cyber-Angriffen und die Prävention von sowie Reaktion auf IT-Sicherheitsvorfälle kümmern.

CERT-Bund

Das CERT-Bund (Computer Emergency Response Team der Bundesverwaltung) ist im BSI angesiedelt und fungiert als zentrale Anlaufstelle für Bundesbehörden zu präventiven und reaktiven Maßnahmen bei sicherheitsrelevanten Vorfällen in Computersystemen.

CERT-Verbund

Der deutsche CERT-Verbund ist eine Allianz mehrerer deutscher Sicherheits- und Computer-Notfallteams von Unternehmen und Behörden.

Cloud/Cloud-Computing

Cloud-Computing bezeichnet das dynamisch an den Bedarf angepasste Anbieten, Nutzen und Abrechnen von IT-Dienstleistungen über ein Netz. Angebot und Nutzung dieser Dienstleistungen erfolgen dabei ausschließlich über definierte technische Schnittstellen und Protokolle. Die Spannbreite der im Rahmen von Cloud-Computing angebotenen Dienstleistungen umfasst das komplette Spektrum der Informationstechnik und beinhaltet unter anderem Infrastrukturen (z. B. Rechenleistung, Speicherplatz), Plattformen und Software.

Command-and-Control-Server/Steuerungsserver

Siehe Bot/Botnetz.

DNS

Das Domain Name System (DNS) ordnet den im Internet genutzten Adressen und Namen, wie beispielsweise www.bsi.bund.de, die zugehörige IP-Adresse zu.

DoS-/DDoS-Angriffe

Denial-of-Service(DoS)-Angriffe richten sich gegen die Verfügbarkeit von Diensten, Webseiten, einzelnen Systemen oder ganzen Netzen. Wird ein solcher Angriff mittels mehrerer Systeme parallel ausgeführt, spricht man von einem verteilten DoS- oder DDoS-Angriff (DDoS = Distributed Denial of Service). DDoS-Angriffe erfolgen häufig durch eine sehr große Anzahl von Computern oder Servern.

Drive-by-Download/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 Webbrowser, in Zusatzprogrammen des Browsers (Plugins) oder im Betriebssystem ausgenutzt, um Schadsoftware unbemerkt auf dem PC zu installieren.

Ende-zu-Ende-Verschlüsselung

Um besonders sensible Informationen sicher per E-Mail zu versenden, können zusätzlich zum Transportkanal auch die Inhalte einer E-Mail verschlüsselt werden. Um diese Ende-zu-Ende-Verschlüsselung verwenden zu können, benötigen Absender und Empfänger einer Nachricht entsprechende Verschlüsselungssoftware, die auf den eingesetzten Rechnern installiert sein muss.

Exploit-Kit

Exploit-Kits (auch Exploit-Packs genannt) sind Werkzeuge für Cyber-Angriffe und werden auf legitimen Webseiten platziert. Mithilfe verschiedener Exploits wird automatisiert versucht, eine Schwachstelle im Webbrowser oder dessen Plug-ins zu finden und zur Installation von Schadprogrammen zu verwenden.

Industrial Control System (ICS)/Industrielle Steuerungssysteme

Systeme zur Fertigungs- und Prozessautomatisierung werden unter dem Begriff Industrial Control Systems (ICS) bzw. industrielle Steuerungssysteme zusammengefasst.

Identitätsdiebstahl

Als Identitätsdiebstahl oder -missbrauch bezeichnet man die Aneignung und unberechtigte Nutzung personenbezogener Daten wie Anschrift, E-Mail-Adresse, Geburtsdatum, Bankkonto- oder Kreditkartennummern im Internet durch Dritte. Ziel eines Angreifers ist es in der Regel, finanzielle Vorteile durch vertrauliche Informationen zu erlangen, in selteneren Fällen auch den rechtmäßigen Identitätsinhaber in Misskredit zu bringen. Identitätsdiebstahl findet vor allem mittels Social Engineering, Schadprogrammen auf infizierten Systemen oder durch Datenabfluss nach dem Hacking von Online-Angeboten statt.

IKT

Abkürzung für „Informations- und Kommunikationstechnik“. Hierunter versteht man die Gesamtheit der Informationstechnik, der Kommunikationstechnik und ihr Zusammenwirken, zum Beispiel in Form von Kommunikationsnetzen.

Industrie 4.0

Industrie 4.0 ist ein Überbegriff für das Zusammenwachsen von realer und virtueller Welt zu einem Internet der Dinge im Hinblick auf die zukünftige Form der Industrieproduktion oder auch der Logistik. Dazu werden Systeme des gesamten Unternehmens untereinander sowie nach innen und außen vernetzt: Maschinen, Sensoren, Produktionsanlagen, Marketing, Vertrieb, Einkauf und Logistik.

Internet der Dinge

Unter Internet der Dinge versteht man die Verknüpfung eindeutig identifizierbarer physischer Objekte mit einer virtuellen Repräsentation in einer internetähnlichen Struktur mittels eines eingebetteten elektronischen Chips.

IS-Revision

Informationssicherheitsrevision (IS-Revision) ist ein Bestandteil eines jeden erfolgreichen Informationssicherheitsmanagements. Nur durch die regelmäßige Überprüfung der etablierten Sicherheitsmaßnahmen und des Informationssicherheitsprozesses können Aussagen über deren wirksame Umsetzung, Aktualität, Vollständigkeit und Angemessenheit und damit über den aktuellen Zustand der Informationssicherheit getroffen werden. Die IS-Revision ist somit ein Werkzeug zum Feststellen, Erreichen und Aufrechterhalten eines angemessenen Sicherheitsniveaus in einer Institution.

Kritische Infrastrukturen/KRITIS

Bei Kritischen Infrastrukturen (KRITIS) handelt es sich um Institutionen und Einrichtungen mit besonderer Bedeutung für das staatliche Gemeinwesen, bei deren Ausfall oder Beeinträchtigung nachhaltig wirkende Versorgungsengpässe, erhebliche Störungen der öffentlichen Sicherheit oder andere dramatische Folgen eintreten würden.

KRITIS-Bereiche

In Deutschland werden derzeit neun Sektoren den Kritischen Infrastrukturen zugeordnet: Transport und Verkehr, Energie, Informationstechnik und Telekommunikation, Finanz- und Versicherungswesen, Staat und Verwaltung, Ernährung, Wasser, Gesundheit, Medien und Kultur.

Logdaten/Logdatei

Eine Logdatei enthält ein Protokoll von Aktionen und Prozessen auf einem Computer.

NTP

Das Network Time Protokoll dient der Zeit-Synchronisation von IT-Systemen in Netzwerken.

NTP-Reflection

Hierbei handelt es sich um eine spezielle Form eines DDoS-Angriffes. Bei einem Reflection-Angriff wird das Opfersystem nicht direkt angegriffen. Stattdessen spielt der Angreifer „über Bande“ (reflection). Dazu sendet er eine Anfrage mit gefälschter Absenderadresse (Opfersystem) an ein Zielsystem (Bande). Die Antwort auf die Anfrage des Angreifers erhält dann aufgrund der gefälschten Adresse nicht der Angreifer, sondern das Opfersystem. Die Antwortpakete sind häufig deutlich größer als die Anfragen. Dadurch ist es dem Angreifer möglich, mit Einsatz einer geringen eigenen Bandbreite viel Angriffsbandbreite zu erzeugen. Man spricht in diesem Fall von einer Verstärkung der eingesetzten Bandbreite.

OpenSSL

OpenSSL ist eine freie Softwarebibliothek, die Verschlüsselungsprotokolle wie Transport Layer Security (TLS) und andere implementiert.

Patch/Patch-Management

Ein Patch („Flicken“) ist ein Softwarepaket, mit dem Softwarehersteller Sicherheitslücken in ihren Programmen schließen oder andere Verbesserungen integrieren. Die Einspielung dieser Updates erleichtern viele Programme durch automatische Update-Funktionen. Als Patch-Management bezeichnet man Prozesse und Verfahren, die helfen, verfügbare Patches für die IT-Umgebung möglichst rasch erhalten, verwalten und einspielen zu können.

Penetrationstest

Ein Penetrationstest ist ein kontrollierter Versuch, von außen in ein bestimmtes Computersystem bzw. -netzwerk einzudringen, um Schwachstellen zu identifizieren. Dazu werden die gleichen

bzw. ähnliche Techniken eingesetzt, die auch bei einem realen Angriff verwendet würden. Er dient dazu, die Erfolgsaussichten eines vorsätzlichen Angriffs einzuschätzen und dadurch die Wirksamkeit der vorhandenen Sicherheitsmaßnahmen zu überprüfen sowie weitere notwendige Sicherheitsmaßnahmen abzuleiten.

Phishing

Das Wort setzt sich aus „Password“ und „fishing“ zusammen, zu Deutsch „nach Passwörtern angeln“. Der Angreifer versucht, über gefälschte Webseiten, E-Mails oder Kurznachrichten an persönliche Daten eines Internetnutzers zu gelangen und damit Identitätsdiebstahl zu begehen.

Plug-in

Ein Plug-in ist eine Zusatzsoftware oder ein Softwaremodul, das in ein Computerprogramm eingebunden werden kann, um dessen Funktionalität zu erweitern.

Ransomware

Ransomware sind Schadprogramme, mit deren Hilfe ein Eindringling eine Zugriffs- oder Nutzungsverhinderung der Daten sowie des gesamten Computersystems erwirkt. Meist dient dies dazu, Lösegeld („ransom“) zu erpressen.

Shell

Als Shell bezeichnet man eine Software, die als Schnittstelle zwischen Mensch und Maschine fungiert. Im Sprachgebrauch etabliert hat sich Shell als Bezeichnung für den Kommandozeileninterpreter, aber auch grafische Benutzeroberflächen wie der Windows Explorer oder der Apple Finder sind Shells.

Social Engineering

Bei Cyber-Angriffen mittels Social Engineering versuchen Kriminelle ihre Opfer dazu zu verleiten, eigenständig Daten preiszugeben, Schutzmaßnahmen zu umgehen oder selbstständig Schadcodes auf ihren Systemen zu installieren. Sowohl im Bereich der Cyber-Kriminalität als auch bei der Spionage gehen die Täter geschickt vor, um vermeintliche menschliche Schwächen wie Neugier oder Angst auszunutzen und so Zugriff auf sensible Daten und Informationen zu erhalten.

Spam

Unter Spam versteht man unerwünschte Nachrichten, die massenhaft und ungezielt per E-Mail oder über andere Kommunikationsdienste versendet werden. In der harmlosen Variante enthalten Spam-Nachrichten meist unerwünschte Werbung. Häufig enthält Spam jedoch auch Schadprogramme im Anhang, Links zu verseuchten Webseiten oder wird für Phishing-Angriffe genutzt.

SSH

SSH steht für „Secure Shell“ und ist eine Anwendung, mit der eine verschlüsselte Netzwerkverbindung zu einem räumlich entfernten Gerät aufgebaut werden kann.

SSL/TLS

TLS steht für Transport Layer Security (Transportschichtsicherheit) und ist ein Verschlüsselungsprotokoll für die sichere Übertragung von Daten im Internet. Bekannt ist auch die Vorgängerversion SSL (Secure Sockets Layer).

UP KRITIS

Der UP KRITIS (www.upkritis.de) ist eine öffentlich-private Kooperation zwischen Betreibern Kritischer Infrastrukturen, deren Verbänden und den zuständigen staatlichen Stellen.

Twitter

Twitter ist eine digitale Echtzeitanwendung zum Verbreiten von Kurznachrichten.

VDE

Verband der Elektrotechnik Elektronik Informationstechnik e.V.

Watering-Hole-Angriffe

Die Analogie des Begriffs Watering Hole bezieht sich auf ein Wasserloch, das Beutetiere anlockt und somit ein bevorzugtes Revier für deren Jäger ist. Bei dieser Angriffsform werden im Vorfeld Internetseiten gehackt und mit Schadcodes versehen, die von einer Zielperson mit hoher Wahrscheinlichkeit aufgerufen werden. Wird eine dieser infizierten Seiten besucht, installiert sich automatisch ein Schadprogramm (z.B. durch Drive-by-Download).

Webbrowser

Webbrowser sind spezielle Computerprogramme zur Darstellung von Webseiten im World Wide Web oder allgemein von Dokumenten und Daten.

Zero-Day-Exploits

Bei Zero-Day-Exploits wird eine Sicherheitslücke bereits zum Zeitpunkt der Entdeckung durch Kriminelle ausgenutzt. Daher bleibt Anwendern und Entwicklern nur sehr wenig Zeit für die Einleitung von Gegenmaßnahmen.

6 Abbildungs- und Tabellenverzeichnis und Fußnoten

Abbildungsverzeichnis

Abb. 1: Anzahl aller Schwachstellen der gelisteten Softwareprodukte	13
Abb. 2: Qualitativer Spam-Verlauf pro Woche in Deutschland seit Januar 2012	16
Abb. 3: Anzahl Windows-Schadsoftware-Varianten	17
Abb. 4: Beispiel einer Schadprogramm-Infektion per Drive-by-Exploit	17
Abb. 5: Beispiel einer Phishing-Mail – erkennbar an der gefälschten Absenderadresse	19
Abb. 6: Beispiel einer Phishing-Webseite – erkennbar an der gefälschten URL	19
Abb. 7: Vorgehensweise bei einem APT-Angriff	21
Abb. 8: Angriffsvektoren auf Mobilkommunikation	23
Abb. 9: Überblick: Ursachen und Wirkung der Gefährdungslage und der Vorfälle	35

Tabellenverzeichnis

Tabelle 1: Auswahl von Softwareprodukten mit hoher Relevanz	13
Tabelle 2: Zusammenfassung der Gefährdungslage der Angriffsmethoden und -mittel	25

Fußnoten

- 1 (Seite 7) BITKOM-Statistik: http://www.bitkom.org/de/markt_statistik/64086_79916.aspx
- 2 (Seite 12) DIVSI: PRISM und die Folgen: Sicherheitsgefühl im Internet verschlechtert;
<https://www.divsi.de/prism-und-die-folgen-sicherheitsgefuehl-im-internet-verschlechtert/>
- 3 (Seite 12) http://www.bitkom.org/de/presse/8477_79728.aspx
- 4 (Seite 12) Umfrage IT-Sicherheit: Kleine Unternehmen sind Risikogruppe (Deutschland Sicher im Netz);
<https://www.sicher-im-netz.de/press/releases/umfrage-it-sicherheit-kleine-unternehmen-sind-risikogruppe>
- 5 (Seite 12) <http://secunia.com/resources/countryreports/de/>
- 6 (Seite 12) Allianz für Cyber-Sicherheit: Cyber-Sicherheitsumfrage 2014, an der sich 257 Unternehmen, Behörden und andere Einrichtungen aller Größenordnungen und Branchen beteiligten.
<https://www.allianz-fuer-cybersicherheit.de/ACS/DE/Micro/Umfrage/umfrage2014.html>
- 7 (Seite 13) <http://secunia.com/resources/countryreports/de/>
- 8 (Seite 13) <http://news.netcraft.com/archives/2014/02/07/are-there-really-lots-of-vulnerable-apache-web-servers.html>
- 9 (Seite 13) <http://developer.android.com/about/dashboards/index.html>
- 10 (Seite 13) gs.statcounter.com/#desktop-os-ww-monthly-201302-201407
- 11 (Seite 15) Vollständige Beschreibung der Bedrohungen und Lösungsansätze im Dokument „Industrial Control System Security - Top 10 Bedrohungen und Gegenmaßnahmen 2014“;
https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_downloads/techniker/hardware/BSI-CS_005.html
- 12 (Seite 17) <http://www.google.com/transparencyreport/safebrowsing/malware/?hl=de>
- 13 (Seite 18) Das BSI weist erneut auf breitflächige Verteilung von Schadprogrammen über Werbefbanner hin; https://www.bsi.bund.de/DE/Presse/Pressemitteilungen/Presse2013/Verteilung_von_Schadprogrammen_ueber_Werbebanne_05042013.html
- 14 (Seite 20) Allianz für Cyber-Sicherheit: Cyber-Sicherheitsumfrage 2014, an der sich 257 Unternehmen, Behörden und andere Einrichtungen aller Größenordnungen und Branchen beteiligten.
- 15 (Seite 21) Das Domain Name System (DNS) ordnet den im Internet genutzten Namen, wie z. B. www.bsi.bund.de, die zugehörige IP-Adresse zu.
- 16 (Seite 21) Das Network Time Protocol (NTP) dient der Zeit-Synchronisation von IT-Systemen in Netzwerken.
- 17 (Seite 24) http://www.bka.de/DE/Presse/Pressemitteilungen/Presse2014/140827__BundeslagebildCybercrime.html
- 18 (Seite 24) Weiterführende Informationen zum Thema Spionage und Wirtschaftsspionage im Verfassungsschutzbericht 2013 des Bundesamtes für Verfassungsschutz.
<http://www.verfassungsschutz.de/de/oeffentlichkeitsarbeit/publikationen/verfassungsschutzberichte/vsbericht-2013>
- 19 (Seite 26) Studie: Industriespionage 2014; http://www.corporate-trust.de/pdf/CT-Studie-2014_DE.pdf
- 20 (Seite 38) https://www.bsi-fuer-buerger.de/BSIFB/DE/Wissenswertes_Hilfreiches/Service/Checklisten/Massnahmen_gegen_Internetangriffe.html;
https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/kataloge.html

Impressum

Herausgeber

Bundesamt für Sicherheit in der Informationstechnik (BSI)

Bezugsquelle

Bundesamt für Sicherheit in der Informationstechnik (BSI)
Godesberger Allee 185–189
53175 Bonn

E-Mail

bsi@bsi.bund.de

Telefon

+49 (0) 22899 9582-0

Telefax:

+49 (0) 22899 9582-5400

Stand

November 2014

Gestaltung

Serviceplan Berlin

Druck

Druck- und Verlagshaus Zarbock Frankfurt am Main

Texte und Redaktion

Bundesamt für Sicherheit in der Informationstechnik (BSI)

Bildnachweis Titelbild

Fotolia

Grafiken

BSI

Artikelnummer

BSI-LB14503

Diese Broschüre ist Teil der Öffentlichkeitsarbeit des BSI.
Sie wird kostenlos abgegeben und ist nicht zum Verkauf bestimmt.

www.bsi.bund.de