Bundesamt
für Sicherheit in der
Informationstechnik

Fokus IT-Sicherheit 2013

Fokus IT-Sicherheit

Überblick IT-Sicherheitslage:

Die Bedrohung durch eine Vielzahl von Cyber-Gefahren hält unvermindert an. Weder für Bürger noch für Unternehmen und Behörden sinkt die Angriffslast. Nach Erkenntnissen des BSI nehmen Angreifer verstärkt die Wirtschaft ins Visier, wobei gerade auch mittelständische Unternehmen in besonderem Maße von Wirtschaftsspionage, Konkurrenzausspähung aber auch Erpressung betroffen sind. Als dominierendes Motiv für Internetangriffe gelten daher nach wie vor finanzielle Beweggründe. Darüber hinaus haben auch Sabotage und der Versuch politischer Einflussnahme durch Hacktivismus im Motivspektrum der Täter deutlich an Gewicht gewonnen. Der Einsatz von Angriffswerkzeugen auch durch nicht professionell agierende Akteure wird durch günstigere Beschaffungskosten leichter möglich.

Abseits der Masse an Standardangriffen auf IT-Systeme von Privatnutzern, Behörden und Unternehmen, ist eine gesteigerte Zielorientierung, eine weitere Professionalisierung der Angreifer und eine damit gesteigerte Qualität der Angriffe zu beobachten.

Mehrstufige Angriffe kombinieren verschiedene Angriffsarten, um sich dem eigentlichen Ziel schrittweise zu nähern. In einigen Fällen wird sogar eigens eine neue Schadsoftware mit speziellen Funktionen konstruiert – etwa zur Tarnung oder um nach dem Angriff Spuren zu verwischen. Keine Ausnahme, sondern die Regel ist dies in professionell ausgeführten, langfristig ausgelegten und umfassenden Cyber-Angriffen – den sogenannten Advanced Persistent Threats (APT).

APTs bedrohen die Wettbewerbsfähigkeit der deutschen Industrie durch gezielte Wirtschaftsspionage oder Konkurrenzausspähung. Das BSI geht davon aus, dass heute mindestens jedes international aufgestellte Unternehmen in Deutschland ein potenzielles APT-Ziel ist. Zudem ist durch Cyber-Sabotage ein Angriff auf Kritische Infrastrukturen, die für das Gemeinwohl unverzichtbare Dienstleistungen erbringen, theroretisch denkbar.

* CERT = Computer Emergency Response Team

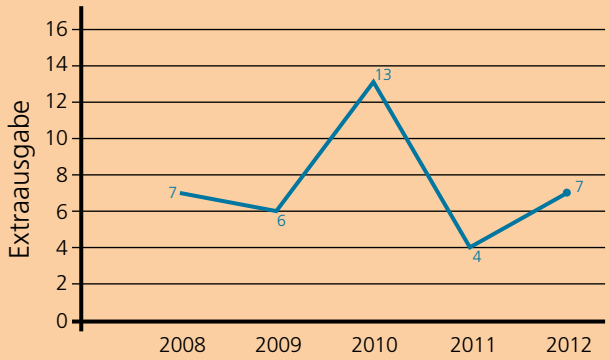
70 E-Mails mit Malware gehen pro Stunde im deutschen Regierungsnetz durchschnittlich ein.

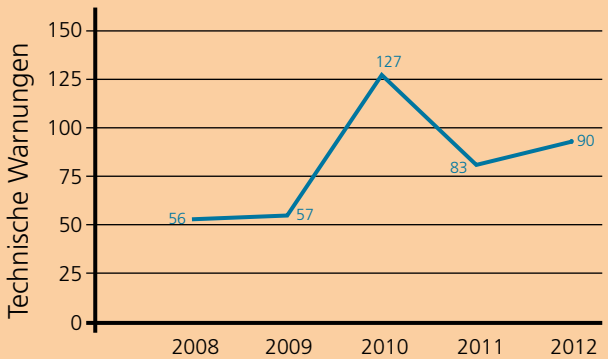
Das BSI beobachtet **pro Tag 5 gezielte Spionageangriffe** auf die Bundesverwaltung.

Rund **30.000 Zugriffsversuche** aus dem Regierungsnetz auf Webseiten, die böswillig manipuliert wurden, werden jeden Monat verhindert.

150 Prozent: Zuwachs von Anfragen betroffener Privatanwender an das Bürger-Servicecenter des BSI seit 2010.

Anzahl der vom Bürger-CERT gemeldeten zeitkritischen Sicherheitslücken und der von CERT-Bund* versendeten „Technischen Warnungen".





Quelle: BSI

97 Schwachstellenwarnungen gab das BSI 2012 heraus – darunter monatlich ein bis zwei **hochkritische Zero Day Exploits**, die bereits am Tag der öffentlichen Bekanntmachung und häufig auch schon viele Tage vorher für Angriffe ausgenutzt wurden.

Das BSI beobachtet einen Anstieg von individuell zugeschnittenen und raffiniert getarnten E-Mails, mit denen die anvisierten Opfer zum Öffnen des Dateianhangs verleitet oder auf eine manipulierte Webseite gelockt werden sollen. Das dafür nötige Vorwissen über ihr Opfer sammeln Angreifer häufig auf den Webseiten von Unternehmen oder in Sozialen Netzwerken. Bei persönlicher Ansprache und oft gefälschten, aber vertrauenswürdig erscheinenden Inhalten sind IT-Anwender schneller bereit, auf einen scheinbar harmlosen Link zu klicken. Mangelnde Sensibilisierung im Umgang mit persönlichen und auch betrieblichen Informationen in Sozialen Netzwerken birgt nach Einschätzung des BSI dabei fast ebenso große Risiken wie technisch veraltete Systeme.

Schadsoftware wird auch nach wie vor massenhaft ungezielt verbreitet. Längst tot geglaubt, erlebt das Phishing, bei dem potenzielle Opfer per Link in einer E-Mail auf eine gefälschte Webseite gelockt werden, derzeit ein Comeback. Die durchschnittliche Lebenszeit von Phishing-Webseiten ist zwar auf ein Rekordtief abgesunken, die Anzahl solcher Seiten aber im Gegenzug wieder deutlich angestiegen.

Gefährdungsbarometer

Entwicklung von Bedrohungen nach Einschätzung des BSI

Bedrohung	2011	2013	Prognose
DDoS	→	↗	↗
Botnetze	↗	→	→
Drive-By-Exploits	↗	↗	→
Schadprogramme	↗	↗	↗
Identitätsdiebstahl	↗	→	→
Spam (Unerwünschte E-Mails)	→	↘	→

↗ steigend ↘ sinkend → gleichbleibend hoch/niedrig

Quelle: BSI

Die Top 6 Cyber-Gefährdungen

In der Praxis verwenden Angreifer selten nur ein einzelnes Tool, sondern kombinieren mehrere Werkzeuge. In Deutschland schätzt das BSI derzeit die folgenden sechs Gefährdungen als besonders relevant ein. *(Reihenfolge spiegelt keine Rangordnung wider)*

1 DDoS-Angriffe mit Botnetzen, um die Erreichbarkeit von Webservern zu stören oder die Netzanbindung der betroffenen Institution zu unterbrechen.

2 Gezieltes Hacking von Webservern, um dort Schadsoftware zu platzieren oder weitergehende Spionageangriffe in angeschlossenen Netzen oder Datenbanken vorzubereiten.

3 Drive-by-Exploits z.B. auch in Werbebannern zur breitflächigen Schadsoftware-Infiltration beim Surfen mit dem Ziel, die Kontrolle über die betroffenen Rechner zu übernehmen.

4 Gezielte Schadsoftware-Infiltration mithilfe von Social Engineering über E-Mail mit dem Ziel der Kontrollübernahme des betroffenen Rechners und anschließender Spionage.

5 Ungezielte Verteilung von Schadsoftware via Spam oder Drive-by-Exploits mit Fokus auf Identitätsdiebstahl.

6 Mehrstufige Angriffe, bei denen zum Beispiel zunächst Sicherheitsdienstleister oder zentrale Zertifizierungsstellen kompromittiert werden, um in weiteren Schritten dann die eigentlichen Ziele anzugreifen.

Jeder dritte Deutsche (34 Prozent) besitzt ein Smartphone.[1] Aufgrund der stark anwachsenden Zahl der mobilen Zugänge zu Unternehmensnetzen richten sich Attacken in jüngster Zeit auch verstärkt auf mobile Endgeräte wie Smartphones und Tablets. Die Nutzung von Privat-Geräten für berufliche Zwecke, die unter dem Stichwort „Bring Your Own Device" (BYOD) Einzug in Unternehmen hält, erschwert die Durchsetzung einheitlicher Sicherheitsstandards, wie z.B. ein durchgängiges Patch-Management.

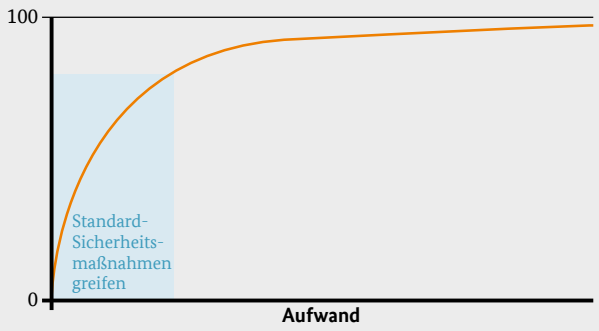
1 Bitkom 2012

Aufwand vs. Sicherheit

Die Masse der Angriffe kann nur erfolgreich sein, wenn Anwender elementare Sicherheitsvorkehrungen, wie aktuelle Updates der Softwareanwendungen und des Betriebssystems, nicht beachten: Nach Erkenntnissen des BSI gelingen Spionageangriffe auch heute noch mit relativ alten Exploits etwa aus dem Jahre 2010.

Generell gilt, dass mit den vom BSI empfohlen Sicherheitsmaßnahmen ein Großteil der massenhaften Cyber-Angriffe erfolgreich abgewehrt werden können. Lediglich ein niedriger Prozentsatz der Angriffe – unter anderem die besonders ausgeklügelten und individualisierten Advanced Persistent Threats – erfordern darüber hinausgehende maßgeschneiderte Maßnahmen.

Schema: Aufwand/Sicherheit



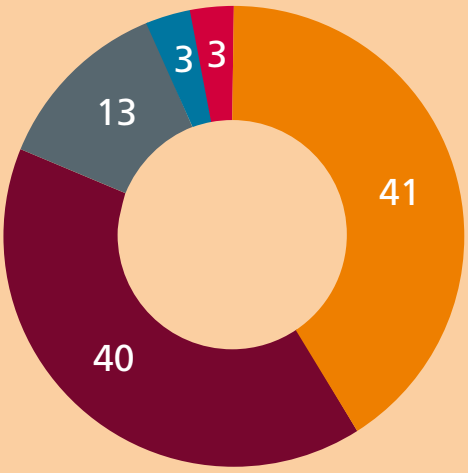
Hundertprozentige Sicherheit ist auch mit noch so hohem Aufwand nicht zu erreichen. Mit überschaubarem Aufwand kann jedoch ein Großteil der Angriffe abgewehrt werden.

Computer-Kidnapping

Mit einem Schadprogramm sperren die Täter die Opfercomputer und nehmen sie quasi in Geiselhaft. Sie verlangen Lösegeld. Um den Anschein offener Erpressung zu vermeiden, firmiert eine gefälschte Webseite unter dem Namen einer möglichst vertrauensvoll erscheinenden Institution – zum Beispiel im Namen des Bundeskriminalamtes, des BSI oder der Gesellschaft zur Verfolgung von Urheberrechtsverletzungen (GVU). Die meist per Drive-by-Exploit eingeschleuste Schadsoftware bringt eine Meldung, die dem Nutzer eine vermeintliche Rechtsverletzung vorwirft und zugleich bestimmte Computerfunktionen blockiert. Nach der Zahlung eines Bußgeldes werde der PC wieder entsperrt. Die geforderten Beträge bewegen sich meist zwischen 20 und 100 Euro. Sie sollen auf anonymem Wege beispielsweise per Paysafecard oder Ukash entrichtet werden. Die Anfragestatistik des BSI-Servicecenters zeigt, dass diese Taktik leider nach wie vor sehr erfolgreich ist. Mehr als zehntausend Anfragen und Meldungen gingen dazu von betroffenen Bürgern beim BSI ein.

Statistisch betrachtet ist jede 35. deutsche Webseite mit manipulierten Werbebannern verseucht. Ist ein Rechner nicht auf dem aktuellen Sicherheitsstand, kann er beim Besuch einer Website – quasi im Vorbeisurfen und ohne weitere Interaktion – infiziert werden. Auch die Webpräsenzen großer Zeitungen oder Shopping-Portale werden ohne Wissen der Betreiber missbraucht.

Hilfreich für Identitätsdiebe: Über die Hälfte der befragten Internetnutzer vergeben nicht für jeden Online-Dienst ein eigenes Passwort.



(Angaben in Prozent)

- Ich habe für jeden Dienst ein eigenes unterschiedliches Passwort
- Ich habe mehrere unterschiedliche Passwörter, aber ich benutze schon mal nur eines für mehrere Dienste
- Ich habe ein Passwort für alle Dienste, die ich nutze
- Ich habe kein Passwort, ich nutze keinen Dienst
- weiß nicht, keine Angabe

Quelle: TNS Emnid/BSI (2013)

Was macht APTs* so besonders?

- Ziel der Angreifer ist, möglichst umfassenden und langfristigen Zugang zu einem Opfer-Netzwerk zu erhalten, um dort sensible Daten zu stehlen.
- Oftmals nutzen die Angreifer bei APTs eine Kombination aus Social Engineering und technischen Angriffswerkzeugen, um an Informationen zu gelangen oder in Systeme einzudringen.
- APTs werden in der Regel mit eigens auf das jeweilige Opfer zugeschnittenen Schadcode-E-Mails ausgeführt.
- APTs nutzen wenn nötig unbekannte Sicherheitslücken, für die noch kein Sicherheitspatch existiert.
- Für hochwertige Spionageprogramme werden oft auch Funktionen zur Tarnung oder zum Verwischen der Spuren entwickelt. So lange solche Schadprogramme unentdeckt bleiben, spionieren oder sabotieren sie anhaltend und so lange verfügt auch keine Antivirensoftware über eine entsprechende Signatur.
- Durch APTs könnten auch mit marginalem Aufwand die Opfer sabotiert und darüber nachhaltig geschädigt werden.

„Im Jahr 2012 gehörten Hackerangriffe in 42,4 Prozent der Spionagefälle zu den Tatmitteln, 2007 lag dieser Wert noch bei 14,9 Prozent. Auch typische Vorbereitungshandlungen wie der Diebstahl von IT-Equipment und Social Engineering sind auf dem Vormarsch.“

Florian Oelmaier, Leiter IT-Sicherheit und Computerkriminalität, Corporate Trust GmbH

„Allgemein wird die Wahrscheinlichkeit, dass das eigene Unternehmen angegriffen werden kann, unterschätzt.“

Christoph Fischer, Geschäftsführender Gesellschafter, BFK edv-consulting

Schützen - aber wie?

Einsatz vertrauenswürdiger IT, Zertifizierung und Zulassung:

Vor allem in sicherheitskritischen Bereichen sollten ausschließlich Komponenten eingesetzt werden, die sich einer Zertifizierung nach einem international anerkannten Zertifizierungsstandard unterzogen haben.

Verschlüsselungstechnik und Risikobewusstsein:

Zur Wahrung der Vertraulichkeit und Integrität von Informationen, die mittels IKT-Netze übertragen werden, ist der Einsatz von vertrauenswürdiger Verschlüsselungstechnik unerlässlich. Zudem sollte das Bewusstsein bestehen, dass technische Kommunikation potenziell nachvollziehbar ist.

Für weitere Informationen zur sicheren Anwendung von Informations- und Kommunikationstechnik informieren Sie sich unter:

- **www.bsi.bund.de**
- **www.allianz-fuer-cybersicherheit.de**
- **www.bsi-fuer-buerger.de**

* Advanced Persistent Threats

Über das BSI

Das Bundesamt für Sicherheit in der Informationstechnik ist die zentrale IT-Sicherheitsbehörde in Deutschland. Ziel des BSI ist der sichere Einsatz von Informations- und Kommunikationstechnik in unserer Gesellschaft.

Die Angebote der Behörde richten sich dabei an die öffentliche Verwaltung in Bund, Ländern und Kommunen ebenso wie an Wirtschaftsunternehmen und Bürger. Mit Unterstützung des BSI soll IT-Sicherheit bei diesen Zielgruppen als wichtiges Thema wahrgenommen und eigenverantwortlich umgesetzt werden.

Beispielsweise arbeiten im Rahmen der Allianz für Cybersicherheit, einer Initiative von BSI und BITKOM, Unternehmen, Institutionen und Behörden auf freiwilliger Basis zusammen, um Cyber-Sicherheit zu fördern und zu gestalten. Dabei verfolgen sie das Ziel, aktuelle und relevante Informationen flächendeckend bereitzustellen, um den Schutz der von Cyber-Angriffen betroffenen Unternehmen und Behörden zu verbessern.

Das Lagezentrum im BSI beobachtet darüber hinaus eine Vielzahl von gezielten und ungezielten Cyber-Angriffen und zieht daraus Schlussfolgerungen in Bezug auf die Verbesserung der IT-Sicherheit in Deutschland. So erarbeitet das BSI beispielsweise Mindeststandards und Handlungsempfehlungen zur IT- und Internet-Sicherheit.

Der globalen Herausforderung Informationssicherheit stellt sich das BSI durch die aktive Mitarbeit in internationalen Gremien wie zum Beispiel der EU, NATO, OECD und ISO sowie durch bi- und multilaterale Zusammenarbeit mit anderen Staaten.

Juli 2013
Bundesamt für Sicherheit in der Informationstechnik – BSI
Godesberger Allee 185 - 189
53175 Bonn
Tel.: +49 (0) 228 99 9582-0
E-Mail: oeffentlichkeitsarbeit@bsi.bund.de
Internet: www.bsi.bund.de

www.bsi.bund.de

Artikelnumer BSI-IFA13/301