Bundesamt
für Sicherheit in der
Informationstechnik

SENSIBILISIERUNG

Cyber-Bedrohungen – ein Einstieg

Häufig gestellte Fragen und Antworten

Cyber-Angriffe und Cyber-Sicherheit werden derzeit intensiv in der Öffentlichkeit diskutiert. Für Hersteller, Dienstleister und Anwender von Informationstechnik stellen sich in diesem Zusammenhang viele Fragen, insbesondere hinsichtlich der Betroffenheit des eigenen Verantwortungsbereichs. Das vorliegende Dokument greift die wichtigsten und häufigsten Fragen zur Cyber-Sicherheit auf und vermittelt anhand der Antworten einen schnellen Einstieg in das Thema.

Was sind Cyber-Angriffe?

Informationstechnische Systeme (IT-Systeme) werden heute kaum noch isoliert eingesetzt, sondern sind in der Regel global vernetzt. Die Kommunikation zwischen den IT-Systemen erfolgt meist über lokale und globale Netze, beispielsweise über das Internet oder über Mobilfunknetze. Auch werden fast alle Computer, die nicht ständig an ein Datennetz angeschlossen sind, ab und zu mit neuen Informationen versorgt, zum Beispiel wenn neue Datenbestände oder neue Programmversionen mit Hilfe von Datenträgern eingespielt werden.

Die Gesamtheit dieser global miteinander kommunizierenden IT-Systeme wird *Cyber-Raum* (cyber space) genannt. Ein wichtiger Teil des Cyber-Raums ist das Internet, in das immer mehr IT-Kommunikationsbeziehungen verlagert werden. Weltweit werden jedoch auch viele andere Vernetzungsstrukturen genutzt.

Die Möglichkeiten der globalen Vernetzung werden allerdings auch von Tätern für schädliche Aktivitäten missbraucht. Von einem *Cyber-Angriff* (cyber attack) spricht man, wenn der Cyber-Raum als primärer Angriffsweg benutzt wird oder selbst das Ziel eines Angriffs ist. Trotz der großen Anzahl unterschiedlicher Angriffsziele und möglicher Angriffsmethoden kann die Motivation hinter einem Cyber-Angriff häufig auf Geld, Informationsbeschaffung, Sabotage, Einflussnahme oder Durchsetzung politischer Interessen zurückgeführt werden.

Wer sind die Cyber-Angreifer?

Die vorsätzlich handelnden Angreifer im Cyber-Raum lassen sich in folgende Gruppen differenzieren:

- Cyber-Aktivisten: Angreifer, die durch einen Cyber-Angriff auf einen politischen, gesellschaftlichen, sozialen, wirtschaftlichen oder technischen Missstand aufmerksam machen oder eine diesbezügliche Forderung durchsetzen wollen („Hacktivismus“). Die Motivation hinter dem Angriff ist Einflussnahme. Der durch einen Cyber-Angriff entstandene Schaden wird in Kauf genommen bzw. forciert, um eine höhere Aufmerksamkeit zu erlangen. Sogenannte *ethische Hacker* fokussieren sich auf gesellschaftliche oder soziale Themen.
- Cyber-Kriminelle: Die Motivation von Cyber-Kriminellen ist es, mithilfe der Informationstechnik auf illegalen Wegen Geld zu verdienen. Die Bandbreite reicht von organisierter Cyber-Kriminalität bis hin zu einfacher Kriminalität mit geringen Schäden.

- Wirtschaftsspione im Cyber-Raum: Durch die Vorteile des Internets ergeben sich für Spione neue Möglichkeiten. Wirtschaftsspionage und Konkurrenzausspähung dienen finanziellen Interessen. Interne Informationen über Mitbewerber und deren Produkte bieten geldwerte Vorteile im globalen Wettbewerb.
- Staatliche Nachrichtendienste im Cyber-Raum: Cyber-Angriffe durch staatliche Nachrichtendienste dienen – im Gegensatz zur Wirtschaftsspionage – nicht primär finanziellen Interessen, sondern der Informationsbeschaffung und der Einflussnahme.
- Staatliche Akteure im Cyber-War: Im militärischen Sektor wird der Cyber-Raum inzwischen vielfach als weitere wichtige Domäne neben den klassischen militärischen Domänen Land, See, Luft und Weltraum angesehen.
- Cyber-Terroristen: Terroristen können Cyber-Angriffe wie staatliche Akteure und Kriminelle nutzen, um unterschiedliche Ziele anzugreifen und somit ihre Ideologie zu verbreiten und ihren Einfluss auszuweiten.
- Skript-Kiddies: Die Gruppe der Skript-Kiddies führt Cyber-Angriffe durch, um Fähigkeiten und Wissen in der Praxis auszutesten. Es werden keine finanziellen Interessen verfolgt. Die Auswahl der Angriffsziele ist unspezifisch und vielfach allein vom Grad der Absicherung abhängig.

Diese Tätergruppen unterscheiden sich vor allem hinsichtlich ihrer Motivation, Zielsetzungen und Ressourcen. Auf technischer Ebene lässt sich hingegen nicht immer unmittelbar feststellen, welche Tätergruppe hinter einem konkreten Cyber-Angriff steckt.

Warum ist der Cyber-Raum so attraktiv für Täter?

In der Informationsgesellschaft hängt vieles von der schnellen und kostengünstigen Kommunikation über den Cyber-Raum ab, denn immer mehr geschäftliche und gesellschaftliche Prozesse werden dort hin verlagert. Durch diese Entwicklung ist der Cyber-Raum auch für Angreifer immer attraktiver geworden.

Der Cyber-Raum hat eine Reihe von Eigenschaften, die für einen potenziellen Angreifer günstig sind: Räumliche Entfernungen spielen kaum eine Rolle. Der Angreifer kann aus der Ferne agieren, ohne sich vor Ort einem unmittelbaren Risiko auszusetzen. Gerade im Internet bestehen außerdem vielfältige Tarnungsmöglichkeiten für den Täter, da viele Dienste im Internet bewusst offen gestaltet sind.

Besonders Cyber-Kriminelle profitieren davon, dass es im Cyber-Raum mithilfe spezieller Angriffstechniken möglich ist, eine Vielzahl unterschiedlicher Ziele parallel anzugreifen. Selbst wenn ein solcher Angriff nur bei einem geringen Prozentsatz an Zielen tatsächlich erfolgreich ist, entsteht oftmals insgesamt ein erheblicher Schaden. Hierzu trägt auch die starke Verbreitung von Bezahlverfahren und Finanztransaktionen über das Internet bei.

Welche Arten von Cyber-Angriffen gibt es?

Cyber-Angriffe werden häufig anhand des Angriffszwecks kategorisiert, also entsprechend der Wirkung, welche die Angreifer auf den Angriffszielen herbeiführen wollen:

- Angriffe auf die Vertraulichkeit: Die Täter können versuchen, vertrauliche Informationen auszuspionieren, indem sie zum Beispiel ein Funknetz abhören oder gelöschte Informationen wiederherstellen.
- Angriffe auf die Integrität: Manipulationen, zum Beispiel an Informationen, Software oder Schnittstellen, spielen bei vielen Cyber-Angriffen eine wichtige Rolle.
- Angriffe auf die Verfügbarkeit: Die Täter können versuchen, Informationen oder IT-Dienste zu sabotieren, beispielsweise durch verteilte Denial-of-Service-Angriffe (DDoS-Angriffe).

Hierbei ist zu beachten, dass Cyber-Angriffe häufig mehrere Angriffsschritte umfassen, wobei die einzelnen Schritte unterschiedliche Zwecke haben können. Ein Cyber-Angriff mittels eines Spionage-Schadprogramms umfasst beispielsweise zumindest die Installation des Schadprogramms (Angriff auf die Integrität) und den eigentlichen Abfluss von Informationen (Angriff auf die Vertraulichkeit).

Neben dem Angriffszweck können Cyber-Angriffe auch dahingehend unterschieden werden, ob es sich um gezielte Angriffe (ein Ziel oder wenige ausgesuchte Ziele) oder um großflächige Angriffe (möglichst viele beliebige Ziele gleichzeitig) handelt. Diese beiden Angriffsarten sind mit bestimmten Vor- und Nachteilen für den Täter verbunden: Ein breit gestreuter Angriff verspricht z. B. eine höhere Wahrscheinlichkeit, dass

der Angriff zum Erfolg führt. Allerdings fallen derart großflächige Angriffe meist eher auf und provozieren so zeitnahe Gegenmaßnahmen.

Eine umfassende Übersicht der gegenwärtig bekannten Cyber-Angriffsmethoden hat das BSI in der Cyber-Sicherheits-Analyse *Register aktueller Cyber-Gefährdungen und -Angriffsformen*[1] zusammengestellt.

Welchen Schaden können Cyber-Angriffe anrichten?

Typische Angriffsziele im Cyber-Raum sind Informationen, IT-Dienste und IT-Systeme. Der mögliche Schaden, der durch Cyber-Angriffe entstehen kann, richtet sich somit nach dem Wert dieser Ziele für Bürger, Institutionen und die Gesellschaft.

Für den einzelnen Bürger besteht insbesondere die Gefahr, dass er erhebliche finanzielle Verluste durch Cyber-Angriffe erleidet. Manipulationen bei Internet-Bezahlvorgängen oder beim Internet-Banking können dazu führen, dass Geld auf den Konten der Täter landet oder dass das Konto des Opfers leergeräumt wird.

Wirtschaftsspionage und Konkurrenzausspähung sind ein besonderes Risiko für innovative Unternehmen. Durch den Diebstahl von vertraulichen Informationen, etwa aus den Bereichen Produktstrategie oder Forschung und Entwicklung, kann sich ein Konkurrent unter Umständen entscheidende Vorteile verschaffen. Angebotskalkulationen in einem Bieterverfahren oder Vertriebsinformationen sind für Wettbewerber ebenfalls von Interesse. Cyber-Angriffe können auch eine Rolle bei der Erpressung von Unternehmen spielen. Die Täter können zum Beispiel damit drohen, vertrauliche Informationen zu veröffentlichen oder wichtige IT-Dienste, die das Unternehmen für Kunden oder Partner anbietet, für einen längeren Zeitraum zu stören.

Ein besonders hohes Schadenspotenzial besteht bei Angriffen auf die Verfügbarkeit Kritischer Infrastrukturen. Kritische Infrastrukturen sind Organisationen und Einrichtungen mit wichtiger Bedeutung für das staatliche Gemeinwesen, bei deren Ausfall oder Beeinträchtigung nachhaltig wirkende Versorgungsengpässe, erhebliche Störungen der öffentlichen Sicherheit oder andere dramatische Folgen eintreten würden.

Bei der Bewertung des möglichen Schadens ist zu beachten, dass sich Cyber-Angriffe zwar häufig gegen konventionelle Informationstechnik – also beispielsweise Webserver oder Datenbanken – richten, allerdings können auch Systeme zur industriellen Prozesssteuerung / -automatisierung / -leittechnik sowie digitale Mess- / Steuerungs- / Regelsysteme von Cyber-Angriffen betroffen sein. Solche Angriffe können direkte Auswirkungen auf die Sicherheit einer industriellen Anlage haben. Der auch in der Öffentlichkeit intensiv diskutierte Vorfall „Stuxnet“ hat gezeigt, dass dies nicht nur ein theoretisches Szenario ist.

Warum sind Cyber-Angriffe möglich?

Um erfolgreiche Cyber-Angriffe durchzuführen, machen sich Täter vor allem die folgenden Arten von Schwächen zunutze: Software-Schwachstellen, Design-Schwachstellen, Konfigurationsschwachstellen und menschliche Fehlhandlungen. Alle diese Arten von Schwächen lassen sich bei der heutigen Komplexität der Informationsverarbeitung prinzipiell nicht vollständig vermeiden.

- Software-Schwachstellen (Implementierungs-Schwachstellen): Oft können Schwachstellen auf Programmierfehler zurückgeführt werden. Da der Quellcode größerer Software-Produkte mehrere Millionen Programmierzeilen lang sein kann, sind solche Software-Schwachstellen nicht selten.
- Design-Schwachstellen: Anders als Software-Schwachstellen sind Design-Schwachstellen nicht in der konkreten Programmierung einer Software begründet, sondern in der Spezifikation von Funktionsweisen, Schnittstellen, Datenformaten, Übertragungsprotokollen o. ä.

1 https://www.bsi.bund.de/ContentBSI/Themen/Cyber-Sicherheit/Analysen/Grundlagen/BSIa001.html

- Konfigurationsschwachstellen: Software-Produkte lassen sich in der Regel mittels Konfigurationseinstellungen an die jeweilige konkrete Einsatzumgebung anpassen. Solche Einstellungen haben häufig auch Einfluss auf die Sicherheit, sodass durch ungeeignete Konfiguration von Software ebenfalls Schwachstellen entstehen können – zum Beispiel, wenn Sicherheitsfunktionen deaktiviert oder Zugriffsrechte nicht restriktiv genug konfiguriert werden.
- Menschliche Fehlhandlungen: Täter verwenden vielfältige Tricks, um Mitarbeiter zur Mithilfe bei Cyber-Angriffen zu bewegen („Social Engineering"). Zum Beispiel werden verlockende Inhalte in Aussicht gestellt, um die Benutzer dazu zu bringen, auf eine bestimmte Schaltfläche zu klicken oder es werden Sicherheitsprobleme vorgegaukelt, um den Benutzern ihre Passwörter zu entlocken. Oft ist den Mitarbeitern gar nicht bewusst, dass sie zu einem Sicherheitsvorfall beigetragen haben.

Hersteller veröffentlichen oft Aktualisierungen (Patches oder Updates) für ihre Produkte, wenn technische Schwachstellen darin bekannt werden. Dies ist bei Design-Schwachstellen in der Regel schwieriger als bei Software-Schwachstellen. Meist ist es Aufgabe der Benutzer, die Aktualisierungen auf ihren Systemen einzuspielen, um die jeweiligen Schwachstellen zu beseitigen. Verfahren, bei denen Software-Produkte selbsttätig im Internet nach Aktualisierungen suchen und diese gegebenenfalls einspielen, gewinnen zunehmend an Bedeutung.

Um den Zeitraum bis zur Veröffentlichung eines Patches zu überbrücken, werden häufig auch sogenannte Workarounds veröffentlicht. Hierbei handelt es sich um Hinweise, wie durch Änderungen der Konfiguration, der Anwendungsumgebung, der Nutzungsart o. ä. vermieden werden kann, dass die Schwachstelle ausgenutzt wird. Workarounds können auch darin bestehen, bestimmte Funktionen der Software nicht zu nutzen, bis ein entsprechender Patch zur Verfügung steht.

Insgesamt wird der Erfolg von Cyber-Angriffen vor allem durch folgende Faktoren begünstigt:

- In vielen Fällen nutzen Täter technische Schwachstellen aus, bevor sie öffentlich bekannt werden („Zero Day"). Programme, die solche neuen Schwachstellen ausnutzen („Exploits"), werden auf Untergrundmarktplätzen gehandelt.
- In dem Zeitraum zwischen dem Bekanntwerden einer Schwachstelle und dem Erscheinen eines entsprechenden Patches sind viele betroffene Systeme ungeschützt. Workarounds sind oft unbequem oder können aus organisatorischen Gründen nur schwer umgesetzt werden.
- Neu veröffentlichte Updates und Patches werden bei vielen Institutionen erst nach Tagen, Wochen oder überhaupt nicht eingespielt. Dies kann zum Beispiel an mangelnden Ressourcen, organisatorischen Problemen oder an Inkompatibilitäten zwischen verschiedenen Komponenten liegen.
- Informationstechnik und die damit verbundenen Sicherheitsaspekte sind heute so komplex, dass viele Benutzer trotz Sensibilisierung und Schulung mit der Einhaltung der Sicherheitsrichtlinien überfordert sind.

Welche aktuellen Bedrohungen der Cyber-Sicherheit gibt es?

Über Cyber-Angriffe wird zunehmend auch außerhalb der Fachkreise in den Medien berichtet. Große Aufmerksamkeit hat beispielsweise eine Serie von Cyber-Angriffen auf IT-Dienste des Konzerns SONY im Jahr 2011 ausgelöst. Die Täter hatten sich dabei Zugriff auf IT-Systeme verschafft, auf denen große Mengen an Kundendaten gespeichert waren. Im Verlauf der Bewältigung hat SONY umfangreiche Maßnahmen ergriffen, zeitweise wurden auch bestimmte IT-Dienste abgeschaltet.

Erhebliche Folgen hatte auch der Cyber-Angriff auf das niederländische Unternehmen DigiNotar, das als Zertifizierungsstelle sogenannte *TLS/SSL-Zertifikate* herausgegeben hat. Mithilfe solcher TLS/SSL-Zertifikate können IT-Systeme die Identität anderer IT-Systeme, mit denen sie über das Internet kommunizieren, überprüfen. 2011 gelang es dem Täter, sich Zugriff auf Systeme von DigiNotar zu verschaffen und gefälschte Zertifikate zu erstellen. Dies ist ein schwerwiegender Sicherheitsvorfall, da solche gefälschten Zertifikate unter Umständen für vielfältige Folgeangriffe benutzt werden können. Durch Änderungen an zentralen Sperrlisten bzw. durch Software-Updates mussten die Hersteller von Internet-Browsern die gefälschten Zertifikate für ungültig erklären. Nur wenige Wochen nach dem Vorfall war das Unternehmen DigiNotar insolvent.

Dass sich Cyber-Angriffe auch über einen sehr langen Zeitraum erstrecken können, zeigen Berichte über Cyber-Angriffe auf das kanadische Technologieunternehmen Nortel. 2012 wurde bekannt, dass Täter ab dem Jahr 2000 mehrere Jahre lang Cyber-Spionage bei Nortel betrieben haben.

Das Lagezentrum des BSI beobachtet und bewertet die Bedrohungslage im Cyber-Raum kontinuierlich. Auch Analysen der abgewehrten Angriffe auf die Regierungsnetze des Bundes fließen dabei ein. Die folgenden statistischen Informationen zeigen, dass Cyber-Angriffe bei Weitem keine Ausnahmeerscheinung sind:

- Etwa alle zwei Sekunden erscheint ein neues Schadprogramm oder eine neue Variante.
- Pro Minute werden etwa zwei digitale Identitäten in Deutschland gestohlen.
- Pro Tag werden etwa vier bis fünf gezielte Trojaner-E-Mails im Regierungsnetz detektiert.
- Pro Monat werden etwa 40.000 Zugriffsversuche aus dem Regierungsnetz auf schädliche Webseiten blockiert.

Die Analysen des BSI zeigen, dass Cyber-Angriffe in vielen Fällen von hochprofessionellen Tätern mit ausreichenden Ressourcen durchgeführt werden. Die Angreifer verwenden dabei vielfältige, teilweise sehr ausgefeilte Methoden und attackieren unterschiedlichste Ziele.

Studien zeigen, dass durch Cyber-Angriffe enorme Schäden entstehen. Im *Norton Cybercrime Report 2011* kommt die Firma Symantec beispielsweise zu dem Ergebnis, dass in einem Jahr in Deutschland ein direkter finanzieller Schaden von über 16 Milliarden Euro durch Internet-Kriminalität entstanden ist. Die Studie *The Cost of Cyber Crime* von Detica für das Cabinet Office aus dem Jahr 2011 nennt für das Vereinigte Königreich (UK) einen Betrag von 27 Milliarden Pfund.

Was kann man tun, um sich vor Cyber-Angriffen zu schützen?

Zwar gibt es keinen absoluten Schutz, jedoch können Cyber-Angriffe durch geeignete Maßnahmen deutlich erschwert und in ihren Auswirkungen abgeschwächt werden. Neben den präventiven Maßnahmen kommt es dabei auch auf das möglichst frühe Erkennen und auf das professionelle Reagieren im Falle eines Cyber-Angriffs an.

Das BSI hat auf seinen Webseiten eine Vielzahl an Hinweisen und Empfehlungen veröffentlicht. Diese Publikationen werden regelmäßig ergänzt und aktualisiert:

- BSI-Analysen und BSI-Empfehlungen zur Cyber-Sicherheit (https://www.bsi.bund.de/cyber-sicherheit): Auf diesen Themenseiten bietet das BSI Informationen, Hilfestellungen und Aktivitäten zur Cyber-Sicherheit für professionelle Anwender an und informiert über Aktionen und Kooperationen in diesem Bereich.
- IT-Grundschutz (https://www.bsi.bund.de/grundschutz): IT-Grundschutz bietet eine einfache Methode, dem Stand der Technik entsprechende Sicherheitsmaßnahmen zu identifizieren und umzusetzen.

Das BSI empfiehlt allen Unternehmen, Behörden und anderen Institutionen, die Informationsangebote zum Thema *Cyber-Sicherheit* zu nutzen und die notwendigen Maßnahmen für einen angemessenen Schutz vor Cyber-Angriffen zu realisieren.

Wie kann ich mit dem BSI in Kontakt treten?

Bei Fragen zu Kooperationen, Themen und Inhalten rund um die Cyber-Sicherheit wenden Sie sich bitte an:

Bundesamt für Sicherheit in der Informationstechnik
Postfach 20 03 63
53133 Bonn
E-Mail: cs-info@bsi.bund.de

Mit den BSI-Veröffentlichungen publiziert das Bundesamt für Sicherheit in der Informationstechnik (BSI) Dokumente zu aktuellen Themen der Cyber-Sicherheit. Kommentare und Hinweise können von Lesern an **cs-info@bsi.bund.de** gesendet werden.