IS-Penetrationstest

Penetrationstest von IT-Systemen durch das BSI

Einleitung

Bei der Abwehr von Angriffen gegen IT-Systeme und Netze empfiehlt es sich, nicht nur präventive IT-Sicherheitsmaßnahmen umzusetzen. Die Wirksamkeit der umgesetzten IT-Sicherheitsmaßnahmen sollte zusätzlich mit der Hilfe von *IS-Penetrationstests* geprüft werden. Hierbei wird der Weg, den ein potenzieller Angreifer gehen würde, nachvollzogen, um eventuell noch vorhandene Schwächen in den IT-Systemen und Netzen der eigenen Institution aufzuspüren.

Potenzielle Angreifer kennen herkömmliche IT-Sicherheitsmaßnahmen und typische Defizite gut. Sie suchen daher gezielt nach Schwachstellen in den IT-Systemen und Netzen, also beispielsweise nach aktuellen Sicherheitslücken, die bislang noch nicht behoben worden sind. Aber auch schon länger bekannte Lücken, für die noch keine Sicherheitspatches eingespielt wurden, oder konzeptionelle Schwächen in der gewählten IT-Architektur stellen ein lohnenswertes Ziel dar.

Das BSI bietet für Bundesbehörden oder Betreiber Kritischer Infrastrukturen (im Folgenden Institution genannt) die Durchführung von *IS-Penetrationstests* an. Mit diesen Tests kann gezielt nach genau solchen Lücken in Systemen gesucht werden. Zu den gefundenen Schwachstellen wird der untersuchten Institution durch Maßnahmenempfehlungen eine Hilfestellung zur Beseitigung angeboten, damit diese sich besser gegen Angriffe absichern kann.

In dieser Kurzdarstellung wird die Vorgehensweise des BSI bei einem *IS-Penetrationstest* dargestellt.

Angriffspunkte auf Institutionen

Auch weniger im politischen Fokus stehende Institutionen können das Ziel von Angriffen sein. Von Behörden werden beispielsweise Aufträge nach außen gegeben, es werden Gesetze erarbeitet und veröffentlicht, Steuern erhoben, Steuerrückzahlungen berechnet, Gesetzesverstöße verfolgt, personenbezogene Daten verarbeitet und vieles mehr.

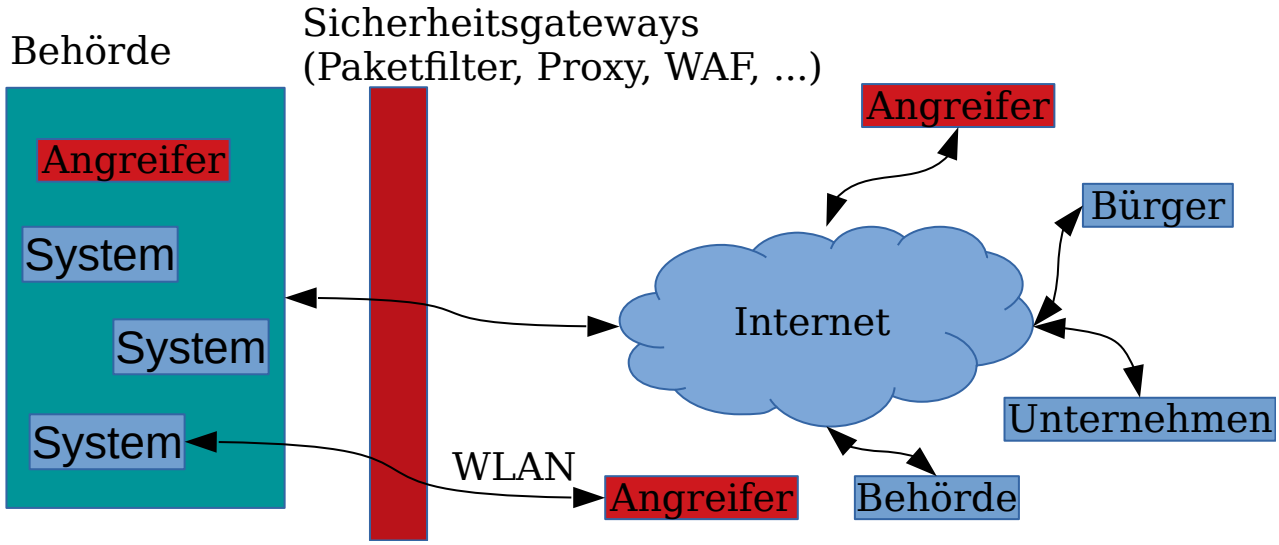

Abbildung 1: Angriffsmöglichkeiten auf Behörden und Institutionen

Kurz gesagt: Behörden sind die Ausführungsorgane des Staates. Das Vertrauen, das die Bürger in die Behörden setzen, ist die Grundlage für viele gesellschaftliche Abläufe.

Und auch Unternehmen besitzen Know-How, auf dem der wirtschaftliche Erfolg des Unternehmens beruht. Hier kann ein Angriff von außen fatale Folgen haben.

Es gibt in jeder Institution sensible Angriffspunkte, über welche die Vertraulichkeit der Daten beeinträchtigt oder die Integrität der Institution untergraben werden kann. Nicht nur ein Datenverlust kann fatal sein, sondern auch der Imageschaden bei einem erfolgreichen Angriff.

Angreifer versuchen auf verschiedene Art und Weise, auf fremde IT-Systeme zuzugreifen. Ein großes Einfallstor für Angriffsversuche ist das Internet. Da die IT-Systeme von Behörden und Institutionen komplex vernetzt sind, ist häufig der Internetzugang einer Institution indirekt auch mit sensiblen Systemen verbunden.

Ein Angreifer könnte aber auch aus dem Inneren einer Institution zuschlagen. Er muss dafür kein Mitarbeiter sein. Ein Angriff könnte beispielsweise über Fremdfirmen, die sich in der Institution aufhalten, oder durch Gäste initiiert werden.

Funknetze sind ein weiterer Angriffspunkt. Beispielsweise könnte eine Institution über ein nicht ausreichend abgesichertes WLAN aus der näheren Umgebung angegriffen werden.

Vorgehensweise

Aus diesen Gründen empfiehlt das BSI, neben den präventiven Sicherheitsmaßnamen auch *IS-Penetrationstests* durchführen zu lassen. Bei einem *IS-Penetrationstest* durch das BSI werden IT-Systeme gezielt auf vorhandene Schwachstellen untersucht.

Das BSI führt hierbei keine destruktiven Tests durch. Möglichen Angreifern ist es nicht immer wichtig, ob die Systeme nach dem Angriff noch funktionieren. Das BSI möchte dies selbstverständlich vermeiden. Angriffe werden daher nur in einzelnen Ausnahmefällen durchgeführt. In der Regel werden für die Tests Audit-Techniken bevorzugt.

Bei diesen Gesprächen untersuchen die BSI-Tester zusammen mit den zuständigen Administratoren die Systeme im festgelegten Umfang und lassen sich die internen Abläufe und Entscheidungen erklären. Dies bietet die Möglichkeit, schnell Fehlkonfigurationen, offene Zugänge oder Verbesserungspotential in den organisatorischen Abläufen zu erkennen. Gleichzeitig erhalten die Administratoren direkt Feedback zu ihren Systemen und können diese nach Abschluss der Tests zielgerichtet verbessern.

Um einen *IS-Penetrationstest* durchführen zu können, wird ein schriftlicher Antrag (gerne auch per E-Mail) benötigt, welcher auf der Homepage des BSI zu finden ist[1]. Der Antrag wird von dem IT-Sicherheitsbeauftragten oder dem IT-Leiter der Behörde unterschrieben. Werden von der zu testenden Anwendung personenbezogene Daten verarbeitet, so müssen der Datenschutzbeauftragte und der Personalrat hinzugezogen werden.

Nach Eingang des Antrags wird ein telefonisches Erstgespräch durchgeführt. Bei dem Gespräch werden die Randbedingungen geklärt. Da die Prüfung jedes einzelnen Systems oftmals nicht mit vertretbarem Aufwand durchgeführt werden kann, werden in den Vorgesprächen die besonders schützenswerten Geschäftsprozesse und Informationen identifiziert. Darauf aufbauend wird gemeinsam überlegt, welche Systeme Angriffsziele sein könnten. Anhand der Netzpläne werden die Schnittstellen identifiziert, über die Angreifer an diese Systeme gelangen könnten. Basierend darauf wird gemeinsam festgelegt, welchen Umfang die Tests einnehmen sollen.

1 https://www.bsi.bund.de/DE/Themen/Cyber-Sicherheit/Dienstleistungen/ISPentest_ISWebcheck/ispentest_iswebcheck.html

Eine ebenfalls wichtige Frage, die im Vorfeld der Tests geklärt werden muss, ist, ob die Systeme selbst oder über einen externen Dienstleister betrieben werden. Ist Letzteres der Fall, so muss dieser in den Auftrag eingebunden werden.

Im Anschluss wird ein Zeitraum (in der Regel rund drei Tage) vereinbart, in dem der *IS-Penetrationstest* durchgeführt werden soll. Es ist wichtig, dass in diesem Zeitraum die Administratoren sowie weitere Ansprechpartner der Behörde bzw. des Hosters vor Ort anwesend sind und für Gespräche zur Verfügung stehen. Nur mit der Hilfe der Administratoren können die Systeme betrachtet und Fragen beantwortet werden.

Ein IS-Penetrationstest vom BSI wird in der Regel in der zu prüfenden Institution „vor Ort" durchgeführt. Sollen nur Webapplikationen über das Internet geprüft werden, so wird hierfür ein sogenannter IS-Webcheck, also ein Sicherheitscheck von Webauftritten durch das BSI, empfohlen.

Die Tests schließen mit einem Bericht ab, in dem die Vorgehensweise und die gefundenen Schwachstellen erläutert werden. Zusätzlich werden Maßnahmenempfehlungen zur Beseitigung der Schwachstellen aufgeführt.

Die Ergebnisse und alle während der Tests gewonnenen Erkenntnisse werden vertraulich behandelt.

Berichterstellung

Der durch das BSI erstellte Bericht enthält Informationen zu den getesteten IT-Komponenten. Zu jeder Komponente werden die gefundenen Schwachstellen genau beschrieben. Darüber hinaus werden geeignete Maßnahmenempfehlungen zur Beseitigung der vorgefundenen Sicherheitslücken bzw. zur allgemeinen/speziellen IT-Sicherheit aufgelistet.

Maßnahmenempfehlung

Das BSI empfiehlt, allgemeine Maßnahmen zur Sicherheit von IT-Systemen in allen Ebenen der installierten IT-Architektur zu implementieren, zu pflegen und entsprechend zukünftigen Erfordernissen weiterzuentwickeln.

Über diese Grundschutzmaßnahmen hinaus können bei einem *IS-Penetrationstest* einige spezifische Schwachstellen gefunden werden, welche die Architektur des getesteten IT-Systeme betreffen. Im Bericht werden zu den Schwachstellen besondere Handlungsempfehlungen gegeben, die den Betreibern helfen sollen, die Sicherheit weiter zu erhöhen.

Abgrenzung

Ein *IS-Penetrationstest* stellt nur eine Momentaufnahme dar, da täglich neue Sicherheitslücken bekannt werden. Bei der Komplexität heutiger Informationsverbünde kann auch mit *IS-Penetrationstests* nicht garantiert werden, dass alle vorhandene Schwachstellen entdeckt wurden. Um nicht nur für den Augenblick die Sicherheit zu erhöhen, wird empfohlen, den *IS- Penetrationstest* regelmäßig (z.B. alle zwei Jahre) zu wiederholen.

Mit *IS-Penetrationstests* können technische und einige organisatorische Schwachstellen aufgedeckt werden, aber selten personellen Gefährdungen. Echte Angreifer nutzen aber auch die Schwachstelle „Mensch" aus, beispielsweise durch Einsatz von sogenanntem Social Engineering. Hierbei gehen Angreifer gezielt auf Mitarbeiter zu und verschaffen sich unter Vorspiegelung falscher Tatsachen Informationen, die den Zugang zu den Systemen ermöglichen. Hierbei wird oft die Hilfsbereitschaft und Gutgläubigkeit der Mitarbeiter ausgenutzt.

Es gibt Sicherheitsprüfungen, bei denen getestet wird, wie weit Angreifer mit Methoden des

Social Engineering kommen würden. Diese Methoden gehören jedoch nicht zum Umfang eines *IS-Penetrationstest*. Das BSI bietet allerdings im Rahmen von Sensibilisierungsveranstaltungen die Möglichkeit an, die Mitarbeiter auf solche Angriffsmethoden vorzubereiten.

Kontakt

Bundesamt für Sicherheit in der Informationstechnik
– Referat CK 13 –
Postfach 20 03 63
53133 Bonn

E-Mail: it-pentest@bsi.bund.de