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 Sicherheitsmaßnahmen umzusetzen, sondern zusätzlich die Wirksamkeit dieser mit Hilfe von *IS-Penetrationstests* („IS“ kurz für Informationssicherheit) zu prüfen. Hierbei wird der Weg, den Angreifende gehen würden, nachvollzogen, um eventuell noch vorhandene Schwächen in den IT-Systemen und -Netzen der eigenen Institution zu detektieren.

Potenzielle Angreifende kennen herkömmliche IT-Sicherheitsmaßnahmen und typische Defizite gut. Sie suchen daher gezielt nach Schwachstellen - 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 Bundes- und Landesbehörden oder Betreibende Kritischer Infrastrukturen (im Folgenden Institution genannt) die Durchführung von *IS-Penetrationstests* an. Mit Hilfe derer kann gezielt nach Schwachstellen in Systemen gesucht werden. Zu den gefundenen Sicherheitslücken 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* beschrieben.

Angriffspunkte auf Institutionen

Behörden sind die Ausführungsorgane des Staates. Das Vertrauen, welches Bürger in die Behörden setzen, ist die Grundlage für viele gesellschaftliche Abläufe.
Und auch Unternehmen besitzen Know-How, auf dem ihr wirtschaftlicher Erfolg beruht. Hier kann ein erfolgreicher Angriff 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 oder die Veröffentlichung sensibler Daten.

Angreifende versuchen auf verschiedene Art und Weise, auf fremde Systeme zuzugreifen. Ein großes Einfallstor ist dabei das Internet. Da die IT-Komponenten von

Behörden und Institutionen komplex vernetzt sind, ist häufig der Internetzugang dieser indirekt auch mit sensiblen Systemen verbunden.

Eine angreifende Entität kann aber auch aus dem Inneren einer Institution agieren, wobei diese dafür kein Mitarbeitender sein muss. Eine Attacke könnte beispielsweise über Angestellte von Fremdfirmen, die sich in der Institution aufhalten, oder durch Gäste initiiert werden.

Funknetze stellen einen weiteren Angriffsvektor dar. Beispielsweise könnte eine Institution über ein nicht ausreichend abgesichertes WLAN (Wireless Local Area Network) aus der näheren Umgebung angegriffen werden.

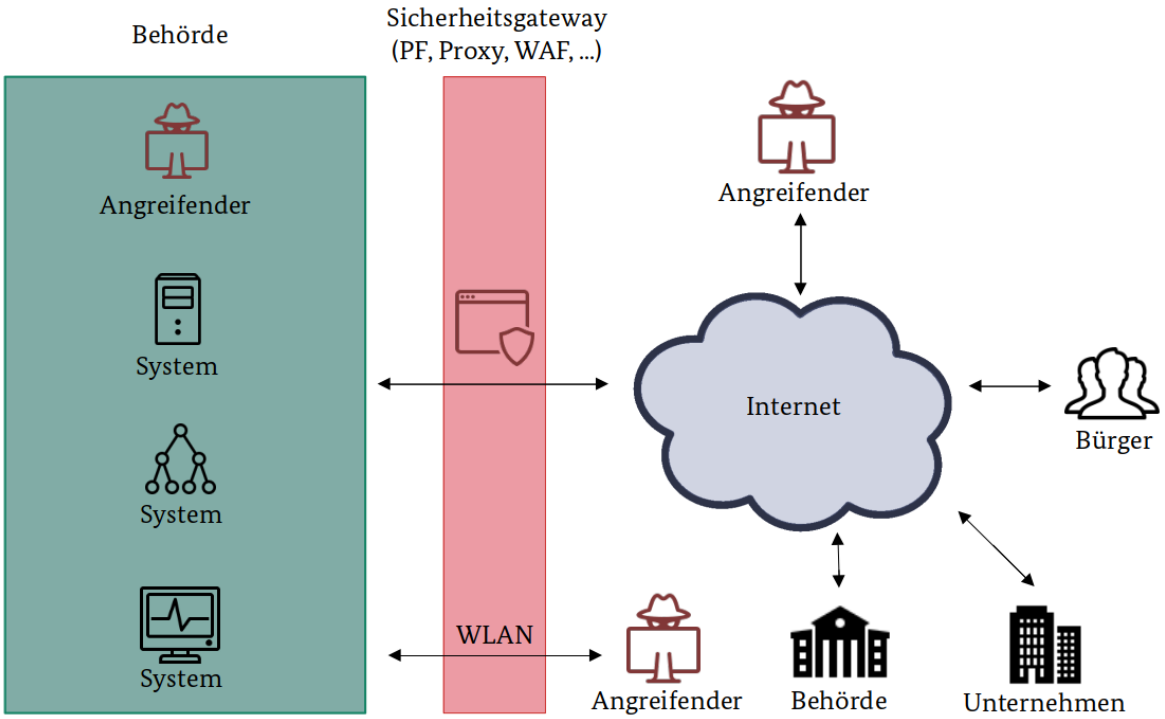

Abbildung 1: Zugriffsmöglichkeiten auf Behörden und Institutionen[1]

Vorgehensweise

Aus diesen Gründen empfiehlt das BSI, neben präventiven Sicherheitsmaßnamen auch *IS-Penetrationstests* durchzuführen. Dabei werden IT-Systeme gezielt auf vorhandene Schwachstellen untersucht. Das BSI führt keine destruktiven Tests durch, obwohl es möglichen Angreifenden nicht immer wichtig ist, ob die Systeme nach dem Angriff noch funktionieren. Das BSI möchte die uneingeschränkte Funktionalität der IT-Komponenten nicht gefährden, weshalb Angriffe nur in einzelnen Ausnahmefällen und

[1]Bildquelle: https://icons8.de/
„PF“ kurz für Paketfilter; „WAF“ kurz für Web Application Firewall

in Absprache mit allen Beteiligten durchgeführt werden. In der Regel werden für die Tests Audit-Techniken bevorzugt.

Im Rahmen des *IS-Penetrationstests* untersucht das BSI-Prüfteam zusammen mit den zuständigen Administrierenden die Systeme im festgelegten Umfang und lässt sich die internen Prozesse erklären. Dies bietet die Möglichkeit, schnell Fehlkonfigurationen, offene Zugänge oder Verbesserungspotenzial in den organisatorischen Abläufen zu erkennen. Gleichzeitig erhalten die Administrierenden direkt Feedback zu ihren Anwendungen und können diese nach Abschluss der Tests zielgerichtet verbessern.

Um einen *IS-Penetrationstest* durchführen zu können, wird ein **schriftlicher Antrag** benötigt, welcher auf der Homepage des BSI zu finden ist[2] und insbesondere per E-Mail gestellt werden kann. Der Antrag wird von der oder dem IT-Sicherheitsbeauftragten, der IT-Leitung oder der Behördenleitung unterschrieben. Werden von der zu testenden Anwendung personenbezogene Daten verarbeitet, so müssen zusätzlich die oder der Datenschutzbeauftragte und der Personalrat hinzugezogen werden.

Vor der Durchführung eines *IS-Penetrationstests* wird ein **Erstgespräch** durchgeführt, um die Rahmenbedingungen und technischen Details zu klären. 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 festgelegt, welche Komponenten Angriffsziele sein könnten. Anhand der Netzpläne werden die Schnittstellen identifiziert, über die angreifende Entitäten an diese gelangen könnten. Basierend darauf wird gemeinsam festgelegt, welchen Umfang die Tests einnehmen sollen.

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

Im Anschluss an den darauffolgenden **Vertragsabschluss** wird ein Zeitraum (in der Regel zwei bis drei Tage) vereinbart, in dem der *IS-Penetrationstest* durchgeführt werden soll. Es ist wichtig, dass in dieser Phase die Administrierenden sowie weitere Ansprechpersonen der Behörde beziehungsweise des Hosters anwesend sind und für Gespräche zur Verfügung stehen. Nur mit der Hilfe der Administrierenden können die Systeme betrachtet und Fragen beantwortet werden.

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

[2]https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Sicherheitsberatung/Pentest_Webcheck/Antrag_Pentest.pdf

Nach Abschluss des *IS-Penetrationstests* wird ein umfangreicher **Bericht** erstellt, der den Beteiligten ausgehändigt wird.

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

Bericht und Maßnahmenempfehlung

Der durch das BSI-Prüfteam erstellte Bericht gliedert sich entsprechend der Kritikalität der gefundenen Schwachstellen. Für jede dieser wird anhand eines Beispiels die davon ausgehende Gefahr beschrieben. Außerdem werden Maßnahmenempfehlungen zur Beseitigung der detektierten Sicherheitslücken beziehungsweise zur Steigerung des allgemeinen/speziellen IT-Sicherheitsniveaus aufgelistet. Dabei werden sowohl fundamentale Grundschutz- als auch individuelle Maßnahmen thematisiert.

Abgrenzung

Ein *IS-Penetrationstest* stellt nur eine Momentaufnahme dar, da täglich neue Schwachstellen bekannt werden. Bei der Komplexität heutiger Informationsverbünde kann auch mit Hilfe von *IS-Penetrationstests* nicht garantiert werden, dass alle Sicherheitslücken tatsächlich gefunden werden. Um das Sicherheitsniveau nicht nur für den Augenblick zu erhöhen, wird empfohlen, den *IS- Penetrationstest* regelmäßig, mindestens alle drei Jahre, zu wiederholen.

Mit *IS-Penetrationstests* können technische und organisatorische Lücken aufgedeckt werden, jedoch selten personelle Gefährdungen. Echte Angreifende nutzen aber auch die Schwachstelle „Mensch“ aus, beispielsweise durch den Einsatz von sogenanntem Social Engineering. Hierbei gehen angreifende Entitäten gezielt auf Mitarbeitende zu und verschaffen sich unter Vortäuschung falscher Tatsachen Informationen, die den Zugang zu den Systemen ermöglichen. Dabei wird oft die Hilfsbereitschaft und Gutgläubigkeit der Angestellten ausgenutzt.

Es gibt Sicherheitsprüfungen, bei denen getestet wird, wie weit Angreifende mit Methoden des Social Engineerings kommen würden. Diese gehören jedoch nicht zum Umfang eines *IS-Penetrationstest*. Das BSI bietet allerdings im Rahmen von Sensibilisierungsveranstaltungen die Möglichkeit, die Mitarbeitenden auf solche Angriffsszenarien vorzubereiten.

Kontakt

Bundesamt für Sicherheit in der Informationstechnik
– Penetrationstests –
Postfach 20 03 63
53133 Bonn

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