Cyber-Sicherheitsrat Deutschland e.V.

Werkzeugkasten Cybersicherheit

Penetrationstest

Definition, Einsatzgebiete & Diskussion

Wir sind wehrhaft

Cybersicherheit erscheint uns oft als unbezwingbare Aufgabe: ein **asymmetrisches Setting**, das Angreifern einen taktischen Vorteil gegenüber Sicherheitsexperten verschafft, wachsende Möglichkeiten und die **Professionalisierung von Cyberkriminellen**, **unklare Zuständigkeiten** und regulatorische Anforderungen bei IT-Sicherheitsinstitutionen und vieles mehr.

Das kann deprimieren.

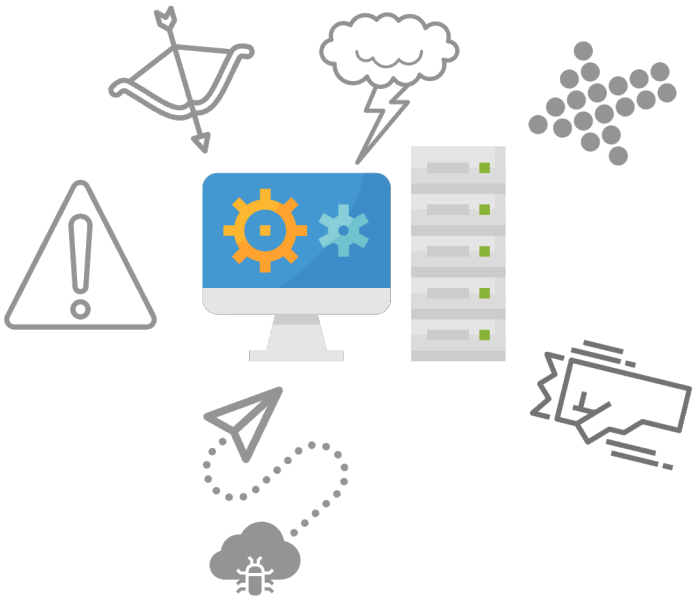
Was wir dabei oft vergessen sind die vielen Menschen, Ressourcen und Werkzeuge auf der anderen Seite, die tagtäglich daran arbeiten, Wirtschaft und Gesellschaft sicherer zu machen. In der Vergangenheit wurden **wirkungsvolle und starke Methoden** entwickelt, die nur an den richtigen Stellen genutzt werden müssen, um Angreifern einen Schritt voraus zu sein.
Es gibt für alles eine Lösung, man muss sie nur finden – vor allem im Bereich Cybersicherheit. Diese Publikationsreihe stellt übersichtsartig die wichtigsten **Methoden im Kampf gegen Cyberattacken** mit ihren Einsatzgebieten sowie Vor- und Nachteilen vor, damit zukünftig die richtigen Werkzeuge an den passenden Stellen parat stehen.

Ich wünsche Ihnen eine anregende Lektüre und interessante Einblicke in den Werkzeugkasten Cybersicherheit.

Hans-Wilhelm Dünn
Präsident
Cyber-Sicherheitsrat Deutschland e.V.

Penetrationstest – Was ist das?

Mit einem Pen(etrations)test versuchen beauftragte IT-SpezialistInnen **in ein Netzwerk oder ein Computersystem einzudringen**, um dieses auf **Schwachstellen** zu untersuchen. Die Methode ähnelt dem Agieren feindlicher Hacker, die Systeme kompromittieren wollen, tut dies jedoch mit **Erlaubnis des Systembetreibers**, um Sicherheitslücken aufzudecken und zu schließen.
Der Pentest ist abzugrenzen vom Schwachstellenscan, der im Gegensatz dazu oberflächlicher, automatisiert und ohne das aktive und kreative Agieren menschlicher Tester abläuft.



Wie läuft ein Pentest ab?

Zu Beginn eines Pentests vereinbart der Systembetreiber mit dem Tester den **Umfang**, die **Ziele** des Tests, die zu verwendenden **Methoden** sowie die **rechtlichen Rahmenbedingungen**.
Anschließend beginnt das **Sammeln von hilfreichen Informationen**, beispielsweise über die verwendete Hard- und Software. Beim darauffolgenden Angriff versucht der Tester mit verschiedenen Techniken, Schwachstellen zu finden und bedient sich dabei den **Methoden, die auch von kriminellen Hackern verwendet werden**.
Werden Schwachstellen gefunden ist es das Ziel, die entsprechenden Zugänge so lange offen zu halten, bis ein **tiefgreifender Zugriff auf das System** möglich ist – analog zu realen Bedrohungen, die oft über einen längeren Zeitraum Systeme infiltrieren, um sensible Daten abzugreifen.
Abschließend folgt eine **Analyse** des Tests mit den Details zu gefundenen Schwachstellen. Dieser dient dazu, das System im Anschluss zu härten. Die genannten Schritte werden in mehreren **Schleifen** wiederholt, um gewonnene Erkenntnisse einzupflegen.

Cyber-Sicherheitsrat Deutschland e.V.

Welche Arten von Pentests gibt es?

Pentests können abhängig vom getesteten System und den vereinbarten Zielen sehr unterschiedlich ausfallen. Unterschieden wird in drei grundsätzliche Arten:
Beim **Black-Box-Test** verfügen Tester über keine oder lediglich wenige Informationen über das Zielsystem. Diese Methode ähnelt der Herangehensweise tatsächlicher Angreifer am meisten. In **White-Box-Test** erhalten die Tester einen umfassenden Zugriff auf Systeminformationen wie Quellcodes oder Anmeldeinformationen und können ihren Test daran orientieren. Zusätzlich gibt es mit dem **Grey-Box-Test** eine Mischform, bei der den Testern ein begrenzter Zugriff auf Informationen eingeräumt wird, beispielsweise auf Netzwerkdiagramme.

Welche Chancen gibt es?

Pentests bieten die Möglichkeit, **Schwachstellen zu entdecken** und zu schließen, bevor feindliche Angreifer dies tun. Sie zeigen auf und ordnen ein, welchem **Risiko** die Zielsysteme ausgesetzt sind. Damit leisten sie einen wichtigen Beitrag zur Integrität und Verfügbarkeit von Systemen. Pentester sind in der Regel **externe ExpertInnen**, die objektiv und unabhängig auf die Cybersicherheit der Kunden blicken und entsprechend fundierte Empfehlungen zur Verbesserung der Sicherheitslage geben können.
Neben den positiven Auswirkungen zur Systemhärtung ist diese Form der Sicherheitsüberprüfung auch vorgeschrieben, um spezifische **Normen** zu erfüllen, wie beispielsweise ISO27001. Da **Social Engineering** ein wesentliches Einfallstor für Cyberkriminelle ist, können Pentests auch um diesen Aspekt erweitert werden.

Welche Risiken gibt es?

Ein Pentest ist **zeit- und kostenintensiv**, trotzdem sollten Kunden nicht am falschen Ende sparen. Fehler von unqualifizierten Pentestern können sehr kostspielig werden, wenn bei dem Eindringen in das System Veränderungen vorgenommen werden, die die Datensicherheit oder die **Verfügbarkeit des Systems beeinträchtigen**.
Neben den professionellen Fähigkeiten kommt es auch auf die Integrität und **Vertrauenswürdigkeit** des Testers an, da dieser mit dem Zugriff auf sensible Daten auch die Möglichkeit erlangt, diese missbräuchlich zu verwenden. Ein Pentest bildet immer eine **Momentaufnahme** des Sicherheitsstands ab. Systemveränderungen und neue Angriffsmethoden sorgen dafür, dass neue Schwachstellen auftreten können.

Cyber-Sicherheitsrat Deutschland e.V.

Wem nutzen Pentests?

Pentests sind für alle **Organisationen** geeignet, die ihre Systeme vor Cyberangriffen schützen und damit ihre Arbeitsfähigkeit sicherstellen wollen.
In bestimmten Bereichen ist der Einsatz weit verbreitet, beispielsweise im **Finanz- und Gesundheitswesen**, da **branchenspezifische Sicherheitsstandards** Pentests vorschreiben.

Fazit

Pentests sind ein wirksames Werkzeug, um eine **Bestandsaufnahme** des aktuellen Sicherheitsstands eines Systems zu erstellen. Dabei sollten sie **nicht im ersten Schritt** eingesetzt werden, da das Eindringen in entdeckte Schwachstellen mit einem hohen Aufwand verbunden ist und beispielsweise Schwachstellenanalysen ebenfalls dafür geeignet sind, eine hohe Zahl von Verwundbarkeiten aufzudecken.
Um eine tiefgreifende Sicherheit zu gewährleisten, sind **regelmäßige** Pentests jedoch unabdingbar, da sie die Methoden von realen Angreifern nachbilden und so eine **Systemhärtung** erwirken können. Bei der Beauftragung sollte darauf Wert gelegt werden, dass eine **trennscharfe Unterscheidung zwischen Pentests und anderen Tools** (z.B. Schwachstellenscan bzw. -analyse) vorgenommen wird.