Schwachstellen der Unternehmens-IT aufdecken – Planung und Durchführung von Penetrationstests

Wie sicher ist Ihre IT wirklich? Nur der neutrale Blick und die fundierte Analyse geben Auskunft.

1. Einleitung

Die Auswirkungen von **Computerkriminalität und Computerbetrug können gravierend** sein, wenn man sein Unternehmen nicht ausreichend schützt oder zu spät auf mögliche Angriffe reagiert. Die IT-Sicherheitsabteilung eines der weltgrößten Softwarehäuser prägte den Satz:

„Es gibt nur zwei Arten von Unternehmen: diejenigen, die wissen, dass sie erfolgreich gehackt wurden und diejenigen, die nicht wissen, dass sie erfolgreich gehackt wurden".

Durch die Dynamik in der Informations- und Kommunikationstechnologie entstehen täglich neue Möglichkeiten für Angreifer, Zugriff auf Unternehmenswerte zu erhalten. Es gibt keine 100%ige Sicherheit für Unternehmen, sich gegen Angriffe auf essenzielle Unternehmenswerte zu wehren. Vielmehr kommt es darauf an, mit abgestimmten Maßnahmen und angemessenem Aufwand die unternehmenskritischen Daten und Informationen bestmöglich zu schützen.

Viele Unternehmen treffen ausgefeilte Maßnahmen, um sich gegen Angriffe von Cyberkriminellen zu schützen. Aber jede Maßnahme ist nur vollständig, wenn deren Wirksamkeit geprüft wurde. Ca. 80% aller erfolgreichen Angriffe auf IT-Infrastruktur erfolgen auf Schwachstellen in IT-Systemen, die älter als 18 Monate sind. Aber auch in etablierten und getesteten Systemen (z.B. in Anwendungen und Firewalls) werden laufend neue Schwachstellen entdeckt und im Internet bekannt gegeben. Eine einmalige Überprüfung schafft nur Sicherheit für den Moment. Um permanent Sicherheit zu schaffen, müssen regelmäßige Überprüfungen stattfinden.

2. Was ist ein Penetrationstest?

Um die Risiken durch einen Cyberangriff einschätzen zu können, ist eine Gefährdungsanalyse - auch unter dem Fachbegriff Penetrationstest - bekannt, notwendig.

Mittels Penetrationstests können einzelne Anwendungen, IT-Systeme oder gar komplette Netzwerke auf Schwachstellen überprüft werden. Dabei wird ermittelt, ob es einem Dritten möglich ist, ein Gerät oder eine Software zu manipulieren oder sensible Daten zu kopieren. Diese Manipulation zielt oft auf Funktionsstörungen oder dem Mitlesen des Datenverkehrs ab. Die Durchführung einer Analyse muss sorgfältig vorbereitet und dokumentiert werden. Wesentlich für einen dauerhaften Erfolg ist die anschließende Umsetzung von Sicherheitsmaßnahmen, die durch den Penetrationstest aufgedeckte Risiken abdecken. Als Beweis bei Nachfragen der Datenschutzbehörden, der Polizei oder Anwälten spielen die Dokumentation und die daraufhin umgesetzten Maßnahmen eine wichtige Rolle im Hinblick auf Verfahren vor Gericht oder bei der Strafverfolgung.

3. Wann sollte ein Penetrationstest durchgeführt werden?

Penetrationstests sollten regelmäßig stattfinden. Je nach Art und Schutzbedarf werden ein oder zweimal pro Jahr diese Tests von einem unabhängigen Dienstleister durchgeführt. Bewährt hat sich der Test der internen Infrastruktur vor Ort im jährlichen Rhythmus, ein Test von Webseiten und anderen aus dem Internet verfügbaren Diensten sollte öfters im Jahr durchgeführt werden.

Der Penetrationstest sollte zudem ein laufender Prozess der IT sein und in die tägliche Arbeit integriert werden. Immer wenn IT-Systeme oder komplette IT-Services eingeführt werden oder grundlegend verändert wurden, sollte in der Folge eine Überprüfung stattfinden. Beispielsweise nach einem Hardwaretausch oder nach der Installation einer neuen Softwareversion bzw. einem Wechsel der eingesetzten Software sollte eine Überprüfung stattfinden. Bei neuen Anwendungen oder Diensten sollte eine Gefährdungsanalyse bereits vor der Inbetriebnahme erfolgen. Einerseits wird damit sichergestellt, dass keine verwundbare Anwendung online gestellt wird. Andererseits stören die Prüfungen den laufenden Produktivbetrieb noch nicht.

4. Warum sollte man einen Penetrationstest durchführen?

Gründe für einen Penetrationstest sind u.a.:

- Absicherung der Unternehmenswerte (z.B. vor finanziellen Schäden, Image- oder Vertrauensverlust von Kunden, Lieferanten und Mitarbeitern)
- Gesetzliche Regularien (z.B. Bundesdatenschutzgesetz, IT-Sicherheitsgesetz)
- Vorgaben von Versicherungen (z.B. Versicherung gegen Auswirkungen von Hackerangriffen)
- Anforderungen und Vorgaben von Kunden

5. Was sind die Ziele eines Penetrationstests?

Zielsetzungen eines Penetrationstests sind:

- Identifikation von Schwachstellen in Anwendungen und Infrastrukturen (z.B. bei Firewalls, Internetauftritt oder in der internen Infrastruktur)
- Minimierung der Risiken für den Unternehmer und das Unternehmen
- Bestätigung der IT-Sicherheit durch einen externen Dritten

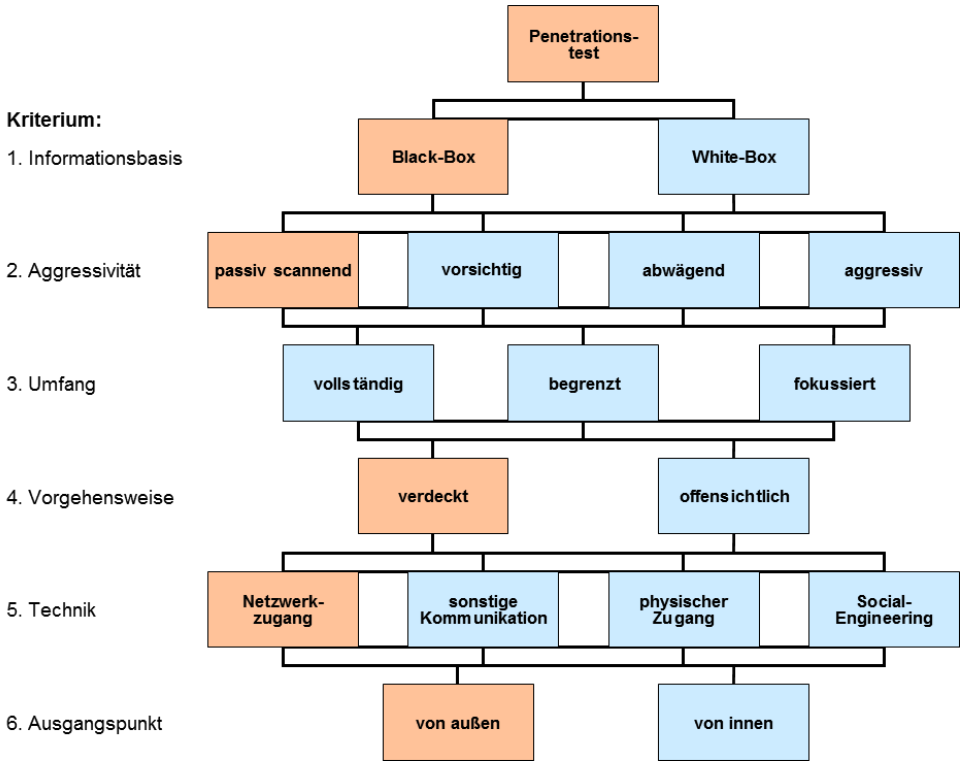
6. Was umfasst ein Penetrationstest?

Ein Penetrationstest umfasst u.a. folgende Bereiche eines Unternehmens:

- Analyse des Gefährdungspotenzials durch externe Angriffe aus dem Internet für Internetauftritte und eCommerce-Plattformen, Portale, Firewalls, etc.
- Analyse des Gefährdungspotenzials durch interne Angriffe auf Anwendungen und Infrastruktur

Penetrationstests können in verschiedenen Ausprägungen durchgeführt werden. Diese reichen von der Simulation eines typischen Internet-Hackers (BlackBox-Test) bis hin zu aufwendigen Tests, die mit Insiderwissen tief in bestehende Infrastrukturen eingreifen (WhiteBox-Test). Dabei wird ein Angriff durch einen Mitarbeiter oder einen externen Dienstleister mit Detailkenntnissen simuliert.

Nachfolgende Grafik erläutert den möglichen Umfang und Vorgehensweisen für einen Penetrationstest:



Bildquelle: BSI Studie Durchführungskonzept für Penetrationstests, Seite 13

Die rot markierten Felder kennzeichnen die typische Vorgehensweise für einen Penetrationstest, bei der ein typischer Internet-Hacker simuliert wird.

7. Was ist das Ergebnis eines Penetrationstests?

Das Ergebnis eines Penetrationstests ist eine Standortbestimmung „Wie ist der aktuelle Stand der Absicherung meiner Daten gegen Cyberangriffe?“ mit

- Darstellung der Schwachstellen
- Risikobewertung der Schwachstellen
- Maßnahmenkatalog zur Behebung der Schwachstellen bzw. zur Minimierung des Risikos, das durch die Schwachstelle entsteht.

8. Wer kann einen Penetrationstest durchführen?

Ein Penetrationstest sollte durch einen unabhängigen, externen Dritten durchgeführt werden. Damit ist ein objektiver Blick auf die Infrastruktur und Organisation gewährleistet. Wichtig ist eine vertrauliche und diskrete Vorgehensweise. Referenzen stehen den ausführenden Unternehmen im Rahmen der Regelung zur Vertraulichkeit meist nicht zur Verfügung. Die Auswahl eines entsprechenden Unternehmens sollte nicht nur von Zertifikaten abhängen, sondern auch durch ein persönliches Kennenlernen getroffen werden. Gefährdungsanalysen sind Vertrauenssache!

9. Wie ist der Ablauf eines Penetrationstests?

Bild: secudor GmbH

Ein Penetrationstest wird über verschiedene Phasen durchgeführt.

Phase 1: Vorbereitung
Im Rahmen der Vorbereitung werden die Rahmenbedingungen für die Durchführung der Gefährdungsanalyse geklärt. Die grundlegende Vorgehensweise wird in einem KickOff-Meeting mit der Geschäftsführung abgestimmt.

- Klärung der Erwartungshaltung und Schaffung eines gemeinsamen Verständnisses
- Festlegung der Verantwortlichkeiten und Ansprechpartner auf Seiten des Auftraggebers und des Auftragnehmers
- Festlegung des Umfangs und der Vorgehensweise
- Festlegung der technischen Rahmenbedingungen für die Durchführung des Tests (Kommunikationswege, Zugriffswege, etc.)
- Festlegung der organisatorischen Rahmenbedingungen (z.B. zeitlicher Ablauf)

Phase 2: Informationsbeschaffung
Nach der Vorbereitung erfolgt die grundlegende Informationsbeschaffung.

- Überprüfung der Zugriffswege
- Sammlung von Informationen über das Zielsystem aus externen Quellen
- Aufwandsanalyse
- Detaillierter Überblick über das Zielsystem

Phase 3: Bewertung und Risikoanalyse
Auf Basis der Informationsbeschaffung folgt eine Bewertung hinsichtlich möglicher Risiken.

- Analyse und Bewertung der Informationen
- Planung der Vorgehensweise
- Festlegung von Schwerpunkten und Prioritäten

Phase 4: Aktiver Angriff
In der vierten Phase wird der aktive Angriff durchgeführt.

- Der Angriff beinhaltet die Ortung, Dokumentation und Bewertung von Schwachstellen.
- Eine aktive Ausnutzung von Schwachstellen wird nur durchgeführt, wenn dies im Rahmen der Vorbereitung vereinbart wurde

Abschlussphase
Die Ergebnisse werden im Rahmen einer Präsentation und eines Abschlussberichtes dokumentiert.

- Präsentation der gefundenen Schwachstellen
- Vorschlag von Maßnahmen, um die Schwachstellen zu beseitigen bzw. um die Risiken zu minimieren
- Abschlussbericht

10. Praktische Hinweise für die Beauftragung eines Penetrationstests bei einem professionellen Unternehmen

- Lassen Sie sich ein Muster eines Abschlussberichts zeigen. Verstehen Sie diesen? Ist dieser für Management und Fachabteilungen (IT) verständlich?
- Wird Ihnen das Vorgehen in verständlicher Art und Weise dargestellt?
- Werden Datenschutzbelange konkret angesprochen und vereinbart?
- Ist der Umfang der Gefährdungsanalyse **genau** definiert?
- Ist der zeitliche Ablauf **genau** vereinbart?
- Ist die IT-Abteilung über die Durchführung einer Gefährdungsanalyse informiert? Die Effizienz eines Tests wird durch die vertrauensvolle Zusammenarbeit mit der Fachabteilung oft erhöht.
- Werden verantwortliche Ansprechpartner für die Dauer der Gefährdungsanalyse auf Seiten des Auftraggebers und des Auftragnehmers festgelegt?
- Fordert der Auftragnehmer eine „Permission to Attack“, mit der Sie, als Handlungsbevollmächtigter, den Umfang, die Zeit und die Verantwortlichkeiten vereinbaren? Professionelle Dienstleister führen ohne diese Erlaubnis keine aktiven Angriffe durch.
- Werden Datenbestände im Unternehmen gesichert (Backups) und sind Vorsorgemaßnahmen für den Ausfall von operativen Systemen getroffen? Im Rahmen eines Penetrationstests können Ausfälle oder Datenverluste entstehen.
- Wurden Eskalationswege / Notruftelefonnummern vereinbart, falls es während der Gefährdungsanalyse zu Beeinträchtigungen des operativen Betriebs kommt?
- Haben Sie mit dem ausführenden Unternehmen eine Vertraulichkeits-Vereinbarung abgeschlossen?
- Erfolgt die Kommunikation (z.B. E-Mail) zwischen Ihnen und dem ausführenden Unternehmen verschlüsselt und vertraulich?
- Wie lange darf eine Gefährdungsanalyse dauern? Beispielhaft kann für einen BlackBox-Test für einen eingegrenzten Bereich 2 bis 3 Manntage für die Durchführung und 1 Tag für die Berichterstellung veranschlagt werden.
- Sind die Kosten für die Gefährdungsanalyse transparent und stimmig? Die Kosten einer Gefährdungsanalyse sind abhängig vom Umfang und von der Dauer sowie von der Qualifikation der eingesetzten Penetrationstester. Für Spezialisten werden entsprechend höhere Tagessätze veranschlagt.

Autoren:
secudor GmbH
Joachim A. Hader
09145 839431, Joachim.Hader@secudor.de

DEXevo GmbH
Klaus Wagner
0821 34320398, klaus.wagner@dexevo.eu

Redaktion:
aitiRaum e.V.
Andrea Henkel

Dieses Merkblatt wurde im Rahmen der Kooperation IT-Sicherheit für Familienunternehmen der IHK Schwaben mit dem Branchennetzwerk aitiRaum e.V. erstellt.

Ansprechpartner:

Anna-Fiora Kilger
Stettenstraße 1 + 3 | 86150 Augsburg
Tel 0821 3162-406 | Fax 0821 3162-342
Anna.Kilger@schwaben.ihk.de