NESEC

Gesellschaft für angewandte Netzwerksicherheit mbH

NESEC LEISTUNGEN

Penetrationstests
Red Teaming

Penetrationstests

dienen der Aufdeckung von Sicherheitslücken in IT-Systemen des Auftraggebers:

„Ein Penetrationstest ist der kontrollierte Versuch, mit den Mitteln und Techniken realer Angriffe in Computersysteme bzw. Netzwerke einzudringen um Schwachstellen zu identifizieren."

Diese vom Bundesamt für Sicherheit in der Informationstechnik (BSI) entlehnte Definition beschreibt den Schwerpunkt eines Penetrationstests, nämlich die Anwendung der Techniken realer Angreifer. Dabei sollen durch die simulierten oder tatsächlich durchgeführten Angriffe Schwachstellen in den IT-Systemen, der Infrastruktur oder der organisatorischen und personellen Sicherheit aufgedeckt werden.
Eine Sicherheitslücke ermöglicht es einem böswilligen Eindringling Informationen unberechtigt zu lesen oder zu verändern oder die Verfügbarkeit der Systeme zu beeinträchtigen. Durch einen Penetrationstest kann geprüft werden, inwieweit die Sicherheit der IT-Systeme durch Bedrohungen von Hackern oder anderen Angreifern gefährdet ist bzw. ob die IT-Sicherheit durch die eingesetzten Sicherheitsmaßnahmen aktuell gewährleistet ist.

Darum sollten Sie einen Penetrationstest durchführen lassen

Die meisten Penetrationstests werden mit dem Ziel in Auftrag gegeben, die Sicherheit der technischen Systeme zu erhöhen. Diese Tests beschränken sich in der Regel auf die aus dem Internet erreichbaren IT-Systeme und Anwendungen, also Firewall, VPN-Zugang, Mailserver, und Webanwendungen. Diese Vorgehensweise ist typisch, wenn in erster Linie geprüft werden soll ob Zugriffe aus dem Internet auf interne Systeme durch unautorisierte Dritte möglich sind.

Die Zielsetzung eines Penetrationstest kann im Vorfeld jedoch auch anders definiert werden. Ein Penetrationstest ist oft zur konkreten Identifizierung von Schwachstellen in neu entwickelten Webanwendungen sinnvoll. Regelmäßig sehen auch Abnahmeverträge von für Unternehmen im Auftrag entwickelten Webanwendungen einen Penetrationstest der Anwendung zur Prüfung der Sicherheit vor.

Eine weitere Zielsetzung kann die Überprüfung der Sicherheit der Infrastruktur durch einen Dritten sein, beispielsweise im Vorfeld einer Zertifizierung nach ISO 27001. Dabei muss jedoch beachtet werden, dass ein Penetrationstest immer nur eine punktuelle Aufnahme der Sicherheit zu einem Zeitpunkt darstellt. Praktisch stündlich werden neue Sicherheitslücken entdeckt und Angriffe entwickelt. Regelmäßige Penetrationstests können jedoch eine Möglichkeit sein, die hohe Sicherheit der IT-Systeme und Daten zu belegen.

Darum Penetrationstests von NESEC

Die Qualität und der Nutzen eines Penetrationstests werden im Wesentlichen davon bestimmt, wie weit dieser auf die individuelle Situation des Auftraggebers eingeht, d. h. wie viel Zeit und Ressourcen auf die Ausforschung von Schwachstellen, die die konkrete IT-Infrastruktur betreffen, verwendet werden und wie kreativ dabei vorgegangen wird. Zur Durchführung der Penetrationstests verwenden wir deshalb nicht nur die gängigen, im Internet und im Handel verfügbaren Schwachstellenscanner, Hacker-Tools und Exploits sondern auch eigenentwickelte Software.
Das Ergebnis des Penetrationstests wird von uns in einem Bericht sowie einer ausführlichen Präsentation dargestellt. Sie beinhaltet die Darstellung der verwendeten Angriffsschemata, aller entdeckten Sicherheitslücken (so vorhanden) sowie eine Bewertung der Gefährdung und enthält Hinweise und Vorschläge zur Verbesserung der Sicherheit der getesteten Systeme. Alle erlangten Kenntnisse und die Ergebnisse des Penetrationstests behandeln wir selbstverständlich vertraulich. Vertrauliche Daten werden von uns nach Übergabe des Berichts und Präsentation der Ergebnisse vernichtet. Wenn Funktionsstörungen der angegriffenen Systeme nicht ausgeschlossen werden können, führen wir Penetrationstests gerne auch außerhalb Ihrer Geschäftszeiten oder am Wochenende durch.

Rahmenbedingungen

Für die professionelle Umsetzung eines möglichen Auftrages ist die Erfüllung folgender Rahmenbedingungen unerlässlich. Sie sichern beide Vertragspartner ab und beugen eventuellem Schaden vor.

- Beiderseitig unterzeichnete Vertraulichkeitsvereinbarung (Non Disclosure Agreement, NDA)
- Auftrag mit unterzeichneter Einverständnis- und Haftungsausschlusserklärung
- Definierte Zielsysteme, Gebäude, Abteilungen bzw. Prozesse
- Definierte Angriffsmethoden und Vorgehensweisen
- Definierter Ansprechpartner beim Kunden
- Schadensvorbeugung, z.B. Backup der definierten Systeme

Unsere Vorgehensweise

Die Vorgehensweise von NESEC zur Durchführung eines Penetrationstests ist grundsätzlich nach dem folgenden, auch vom Bundesamt für Sicherheit in der Informationstechnik empfohlenen Schema aufgebaut:

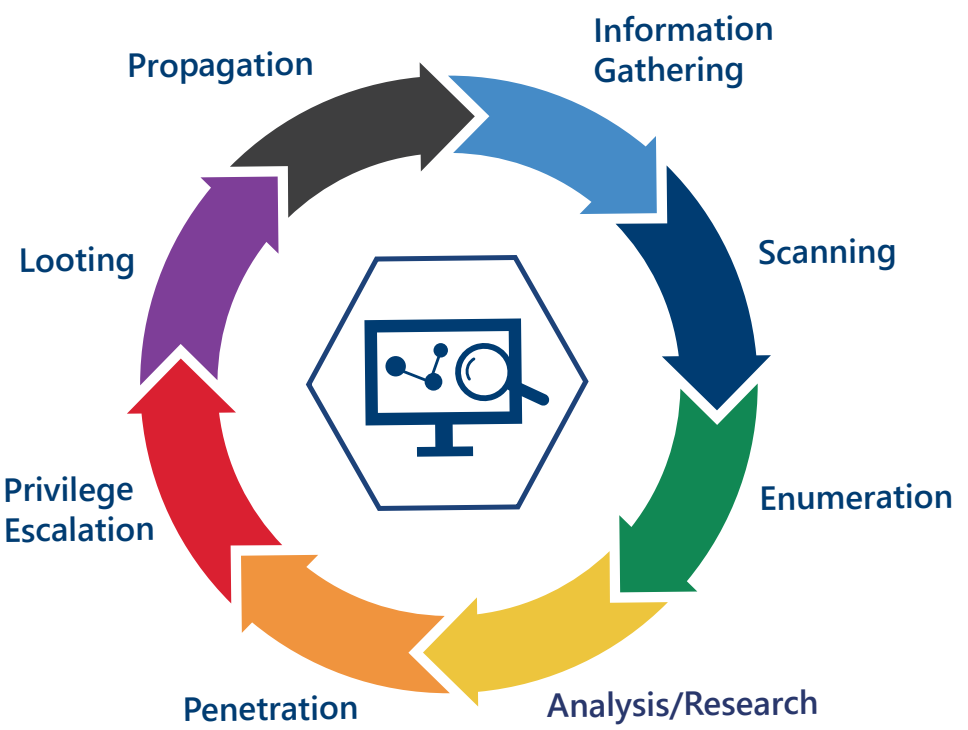
1. Recherche nach Informationen über das Zielsystem
   Im Internet erreichbare Rechner müssen über eine offizielle IP-Adresse verfügen. Frei zugängliche Datenbanken liefern Informationen über IP-Adressblöcke, die einer Organisation zugewiesen sind.
   Auch Suchmaschinen sind eine beliebte Quelle versehentlich veröffentlichter vertraulicher Daten.

2. Scan der Zielsysteme auf angebotene Dienste
   Mit einem Portscanner wird das gesamte Netzwerk geprüft, wobei geöffnete Ports Rückschlüsse auf die zugeordneten Anwendungen zulassen. Aus den gefundenen aktiven Systemen und den offenen Ports lassen sich bereits erste Schlüsse über die Sicherheit treffen.

3. Schwachstellen-Scanning
   Mit verschiedenen Vulnerability Scannern sowie speziellen Web Application Scannern werden die Systeme auf mögliche Schwachstellen hin untersucht.

4. Ausnutzen der Schwachstellen
   Gefundene Schwachstellen können dazu genutzt werden, unberechtigten Zugriff zum System zu erhalten bzw. weitere Angriffe vorzubereiten. Dieses unbefugte Eindringen wird mit „Penetration" bezeichnet.

5. Rechteeskalation und weitere Schritte
   Nach dem Eindringen in ein System erfolgt üblicherweise eine Eskalation der Rechte, um privilegierten Zugriff zu erhalten. Danach könnten von einem echten Angreifer Daten ausgeleitet oder das System als Sprungbrett für weitere Angriffe genutzt werden.

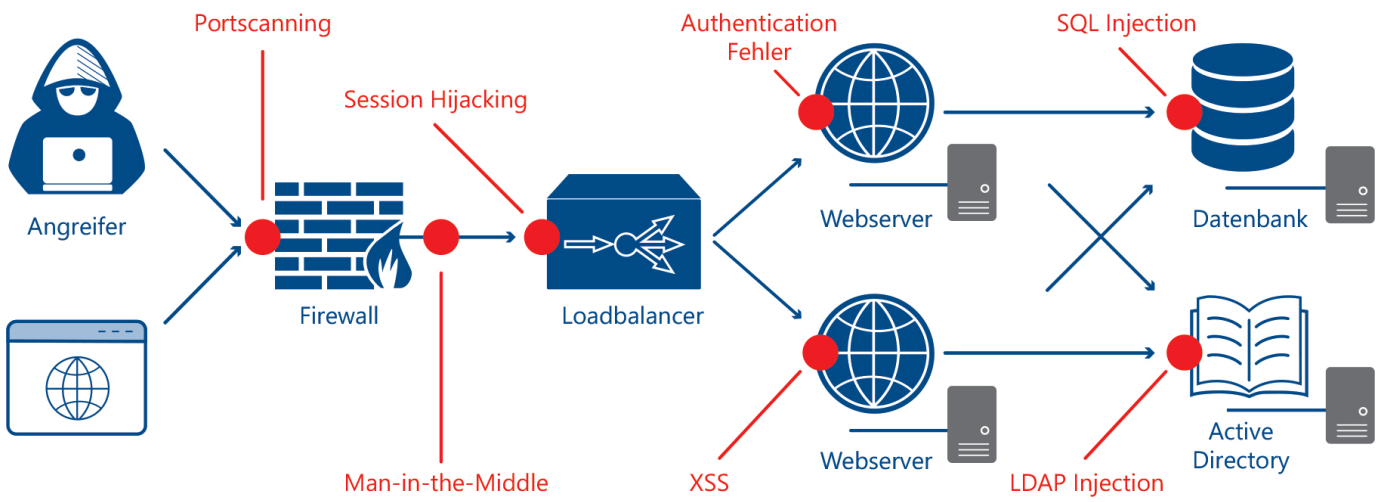


Der konkrete Ablauf hängt von der Zielsetzung des Penetrationstests und den gewünschten, weiter unten beschriebenen Modulen ab und kann deshalb nicht vollständig in der obigen allgemein gültigen Beschreibung dargestellt werden.

Kein rein automatisierter Penetrationstest

Automatisierte Penetrationstests werden überwiegend als günstige Alternative propagiert, werden jedoch noch lange nicht alle Szenarien eines echten Angriffs nachbilden können.
Die meisten automatisierten Penetrationstests kombinieren Vulnerability Scanning mit Exploit Frameworks und ggf. Post Exploitation, d.h. einem auf dem System installierten Agenten, der Rechteeskalation versucht und Daten ausleiten kann. Allerdings können automatisierte Penetrationstests erhaltene Daten und Angriffe bislang noch nicht so zu einer Kill Chain, einer Abfolge von aufeinander aufbauenden Angriffen, kombinieren, wie ein kreativer, erfahrener menschlicher Angreifer.

Ein typisches Szenario ist, dass mit einer ersten Schwachstelle Zugang zu einem System erlangt werden kann, die Rechteeskalation jedoch scheitert und der automatische Penetrationstest deshalb hier abbricht. Ein menschlicher Penetrationstester kann die jedoch bereits erhaltenen Informationen weiter auswerten, den Rechner mit einem anderen Account als Sprungbrett zu einem weiteren System nutzen, auf dem dann die Rechteeskalation möglich ist.
Wir kombinieren deshalb automatisierte Tests mit der jahrelangen Erfahrung unserer Penetrationstester um weitere Angriffe zu finden und alle Risiken angemessen zu identifizieren.



Reproduzierbares Vorgehen

Unsere Vorgehensweise in externen und internen Penetrationstests orientiert sich am Open Source Security Testing Methodology Manual (OSSTMM), wurde von uns jedoch an verschiedenen Stellen vereinfacht und optimiert. Das OSSTMM ist ein offener Leitfaden zur methodischen und vollständigen Durchführung von Sicherheitsanalysen und Penetrations-Tests. Dabei werden alle Aspekte der Kommunikation in Unternehmen betrachtet, wie etwa Sicherheit von TK-Anlagen, Bluetooth, WLAN, Intranet und Internet. Auch der Sicherheit unternehmensinterner Organisation und Prozesse wurden nebst Zutrittskontrollanlagen und Überwachungssystemen eigene Kapitel gewidmet.
Bei der Prüfung von Webanwendungen orientieren wir uns insbesondere am Web Security Testing Guide (WSTG) der OWASP. Speziell die Prüfung von Web-APIs wird jedoch im WSTG noch nicht ausreichend abgedeckt, darum haben wir auch hier unsere konkrete Vorgehensweise optimiert und erweitert.
Selbstverständlich beschreiben wir in unserem Penetrationstestbericht unsere konkrete Vorgehensweise und ermöglichen Ihnen die Nachvollziehbarkeit unserer Ergebnisse.

Ablauf eines externen Penetrationstests
Ein externer Penetrationstest ist in der Regel der erste Schritt zur Prüfung der Resilienz Ihres Unternehmens. Der hier beispielhaft beschriebene Test eignet sich zur Sicherheitsprüfung einer typischen Internet-Anbindung mit einzelnen Systemen in einer DMZ und ggf. extern gehosteten Webservern. Die Prüfung des Webservers z.B. mit Kontaktformular ist enthalten, die Detailprüfung einer komplexen Webanwendung nach OWASP jedoch nicht. Wir beraten Sie gerne und passen den Umfang des Tests an die Bedürfnisse Ihres Unternehmens an.

Ablauf eines externen Penetrationstests

Ein externer Penetrationstest ist in der Regel der erste Schritt zur Prüfung der Resilienz Ihres Unternehmens. Der hier beispielhaft beschriebene Test eignet sich zur Sicherheitsprüfung einer typischen Internet-Anbindung mit einzelnen Systemen in einer DMZ und ggf. extern gehosteten Webservern. Die Prüfung des Webservers z.B. mit Kontaktformular ist enthalten, die Detailprüfung einer komplexen Webanwendung nach OWASP jedoch nicht. Wir beraten Sie gerne und passen den Umfang des Tests an die Bedürfnisse Ihres Unternehmens an.

Ablaufbesprechung / Kickoff

- Telefonisch oder als Videokonferenz
- Abstimmung der Inhalte, generelle Vorgehensweise und Rahmenparameter

Erfüllung rechtliche Rahmenbedingungen

- Beauftragung der NESEC GmbH
- Unterzeichnung Einverständniserklärung, Haftungsfreistellung, Vertraulichkeitsvereinbarung und DSGVO-Auftragsverarbeitung

Externer Penetrationstest der von außen erreichbaren Systeme

- Port- und Schwachstellen-Scan mit verschiedenen Werkzeugen
- Rückmeldung erster Ergebnisse an verantwortliche Administratoren
- Prüfung der Sicherheit von Remote Access Zugängen
- Prüfung der Sicherheit der Mailserver
- Prüfung der Sicherheit der VoIP-Kommunikation
- Prüfung der Angreifbarkeit der selbstbetriebenen Webanwendungen
- Prüfung sonstiger erreichbarer Systeme

Bericht, Dokumentation und Präsentation

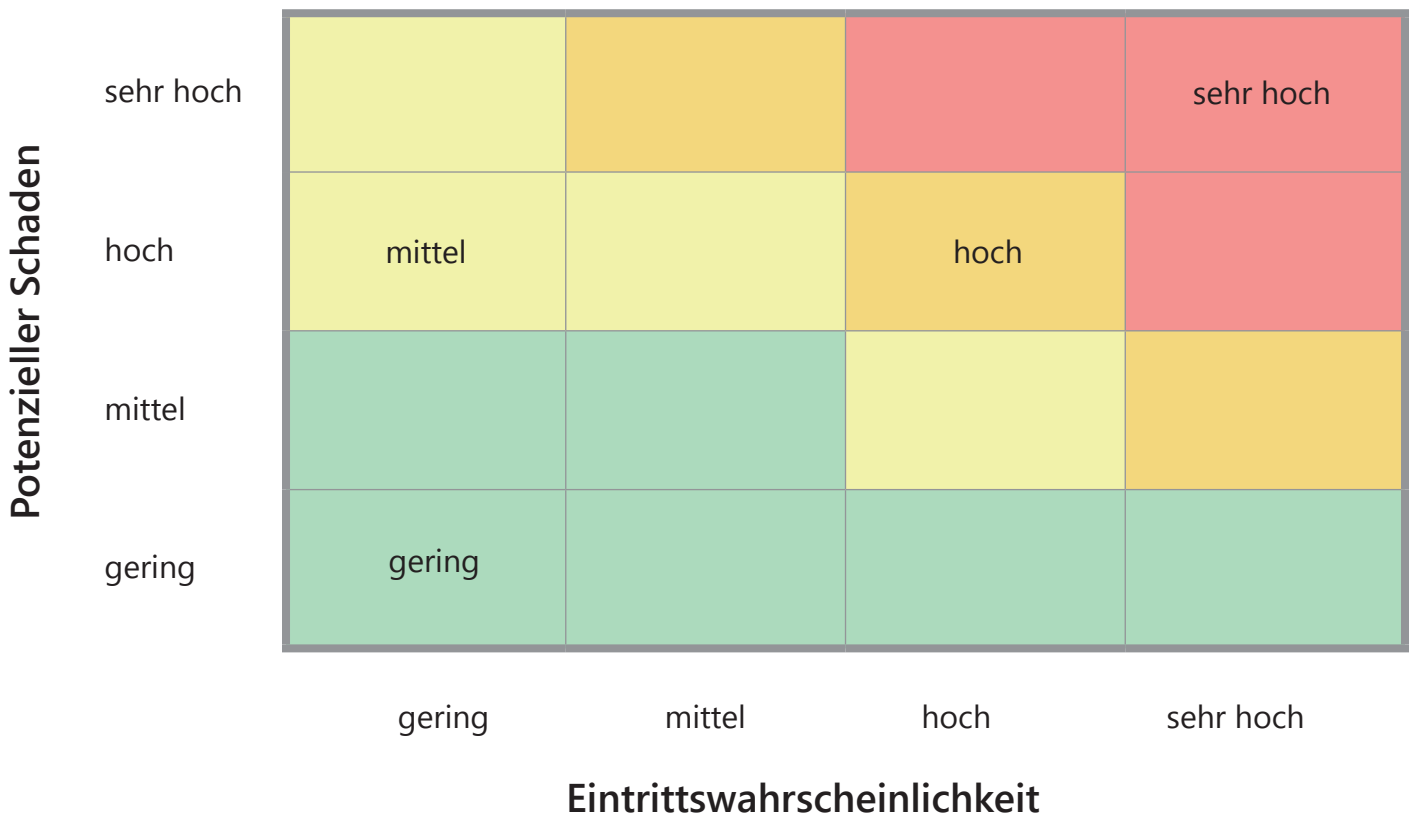
- Erstellung der Dokumentation mit Aufbereitung der gefundenen Schwachstellen
  - Gefundene Schwachstelle
  - Risikobewertung der Schwachstellen
- Verbesserungsvorschläge, Maßnahmenkatalog
  - Handlungsempfehlungen
  - Technische Maßnahmen
  - Organisatorische Defizite
- Management Präsentation

Ausschlüsse

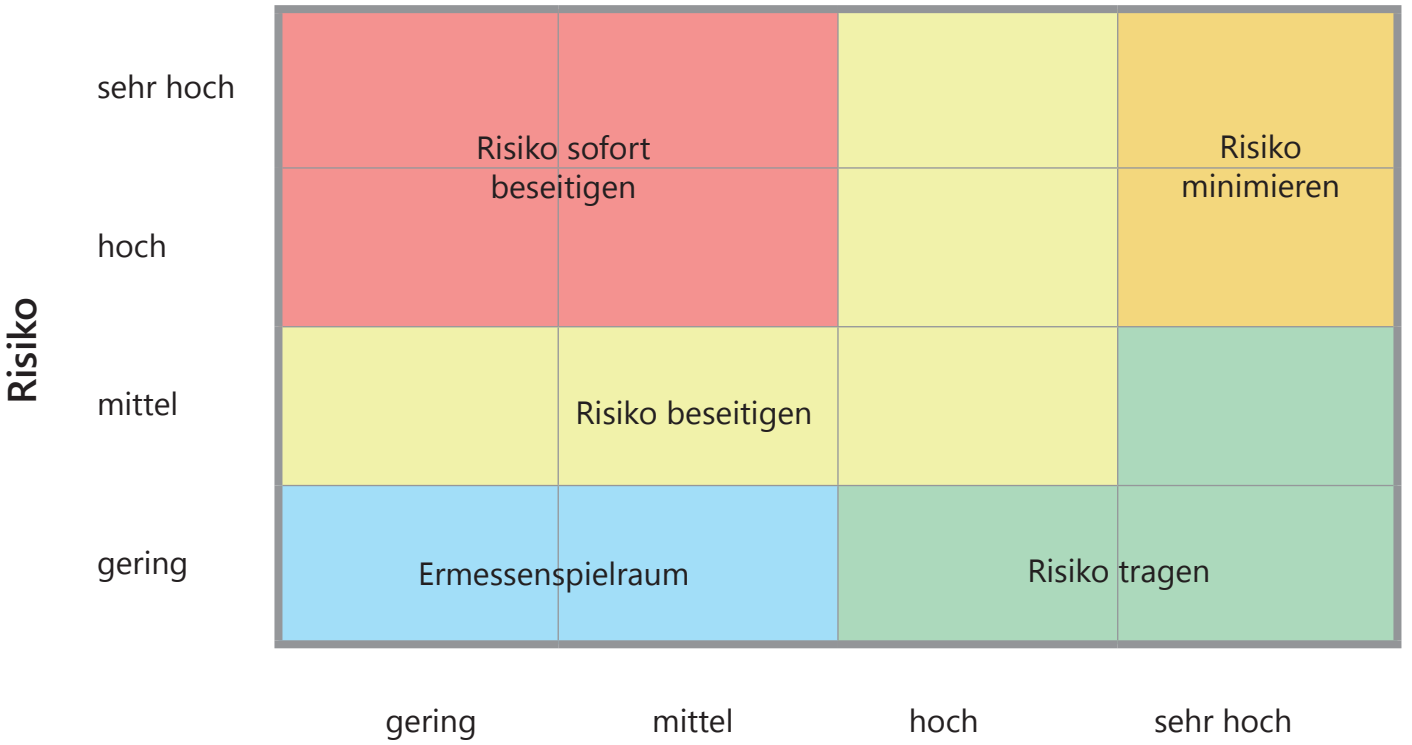
- Es werden keine Social Engineering Angriffe (z.B. Phishing-Mails/Schadcode Mails) durchgeführt
- Es findet keine Prüfung der physischen Sicherheit (Zugangskontrolle, Schließsysteme) statt

Unser Bericht

Im Penetrationstestbericht werden alle Ergebnisse bewertet und eingeordnet. Jede gefundene potentielle Schwachstelle wird selbstverständlich mit Screenshots oder anderen Nachweisen belegt. Außerdem erhalten Sie eine detaillierte Erklärung der konkreten Gefährdungen, möglicher Angriffe die gegen die Schwachstellen denkbar wären sowie Verweise, z.B. auf CVE-Einträge oder auf die MITRE ATT&CK-Matrix. Sie können jede Schwachstelle deshalb leicht verständlich nachvollziehen.
Jede Schwachstelle wird außerdem nach ihrem Risiko bewertet und eine Risiko-Matrix erstellt.
Aus der Beurteilung der Risiken nach Eintrittswahrscheinlichkeit und Schadenspotenzial kann so eine Handlungspriorität abgeleitet werden.



Unsere Risikomatrix verwendet vier Stufen zur Einordnung des potentiellen Schadens sowie der erwarteten Eintrittswahrscheinlichkeit, die nach dem BSI-Standard 200-3 Risikomanagement bewertet werden.
Zusätzlich wird zu jeder Schwachstelle eine Empfehlung zur Beseitigung oder zumindest zur Reduzierung des Risikos angegeben. Die Empfehlungen werden außerdem nach Kosten der Umsetzung bewertet.



Sie erhalten dadurch einen direkten Überblick der vorhandenen Risiken sowie des nötigen Aufwands zur Behebung.

Managementpräsentation

Die abschließende Managementpräsentation erfolgt in Abstimmung mit Ihnen als Sicherheitsverantwortlichen im Unternehmen und dient dazu, innerhalb von ca. zwei Stunden die wichtigsten Ergebnisse des Audits der Geschäftsleitung zu präsentieren. Im Rahmen der Management-Präsentation erhält die Unternehmensleitung einen Überblick über die gefundenen Schwachstellen, die damit verbundenen Risiken, ein „Rating" des Bedrohungspotentials sowie konkrete Handlungsempfehlungen zur Reduzierung oder Beseitigung der Risiken.

NESEC
Gesellschaft für angewandte Netzwerksicherheit mbH
Fürholzener Straße 5a
85386 Eching

Telefon: 089 - 45217100
E-Mail: welcome@nesec.de
Internet: www.nesec.de

NESEC
Gesellschaft für angewandte Netzwerksicherheit mbH