ALLGEIER
CyRis

Whitepaper Penetrationstests

Weshalb braucht Ihr Unternehmen einen Penetrationstest?

Fragen, Daten, Fakten und Hintergründe

Inhalt

I. Vier Punkte, die Sie vorab wissen sollten

1 – Die Notwendigkeit zur Durchführung eines Penetrationstests – rechtliche Aspekte

Seit dem 25. Mai 2018 gelten die Verordnungen der EU-DSGVO. Die DSGVO verfolgt in Bezug auf die technisch-organisatorischen Maßnahmen einen risikoorientierten Ansatz.

In diesem Kontext ermöglichen Penetrationstests die schnelle Erkennung und Beseitigung von IT- und Informationssicherheitslücken, die einen Verlust von personenbezogenen Daten im Sinne der EU-DSGVO zur Folge haben können. Stellen Unternehmen ihre Datenschutzrechtskonformität gemäß DSGVO sicher, profitieren sie von erhöhter Sicherheit für die eigenen Daten. Letztere ist als Wettbewerbsvorteil zu sehen – eine robuste Kopplung von DSGVO und IT-Sicherheit lohnt sich deshalb mehrfach.*

Die typischen Angriffsmethoden, die den Verlust personenbezogener Daten zur Folge haben, sind beispielsweise:

- Identitätsdiebstahl und Datenmissbrauch – fremde Daten werden für betrügerische und kriminelle Aktivitäten erbeutet und genutzt.
- Phishing – durch Täuschung werden persönliche Zugangsdaten zum Beispiel für Online-Banking erbeutet, oft wird dabei mit präparierten E-Mail-Anhängen gearbeitet. 2018 entstand allein durch Phishing für das Online-Banking ein finanzieller Schaden von mehr als 8 Millionen Euro in Deutschland.
- Innentäter-Angriff – Mitarbeiter, die über reguläre Zugriffsrechte verfügen, bringen unbemerkt Daten in ihren Besitz und missbrauchen diese für eigene Zwecke.
- Cyber-Erpressung – beispielsweise durch Ransomware, hier werden unbemerkt Schadprogramme installiert, welche sämtliche Daten verschlüsseln. Danach wird von den Cyberkriminellen eine Lösegeldzahlung für die Entschlüsselung bzw. Wiederherstellung der Daten verlangt.

Die Implementierung von IT-Sicherheitsmaßnahmen gemäß der DSGVO beinhaltet die Notwendigkeit, die eigene IT- und Informationssicherheit auf den neuesten Stand zu bringen. Um diese IT-Sicherheitsmaßnahmen zielgerichtet und effizient umzusetzen, bieten Penetrationstests die optimale Basis.

*Quelle: Datenschutz-Experte.de: DSGVO & Cybersicherheit: Wie wirkt sich die DSGVO auf Datensicherheit aus?

2 – Diese Punkte sollten vor der Durchführung eines Penetrationstests erörtert werden

In einem Vorgespräch zwischen den für Penetrationstests beauftragten IT-Sicherheitsexperten und den Projektverantwortlichen Ihres Unternehmens werden zunächst das Ziel und der Prüfungsgegenstand des Penetrationstests definiert.

Welche Systeme sollen auf Sicherheitslücken überprüft werden - öffentlich verfügbare Dienste wie Ihr Webserver (Portale, Webseite oder Shopsysteme), Mailserver oder Mitarbeiterzugänge, das WLAN oder das gesamte Unternehmensnetzwerk? Möchten Sie wissen, ob bestimmte Compliance-Vorgaben eingehalten werden? Funktioniert Ihr Patch-Management?

Die Zielvorgaben können in die unterschiedlichsten Richtungen gehen – und müssen aus diesem Grund exakt geplant und formuliert werden.

Im Rahmen des Vorgesprächs werden neben den Überprüfungsszenarien und Umfang auch die Handlungsgrenzen definiert. In diesem Zusammenhang ist wichtig zu wissen, dass sich bestimmte Sicherheitslücken nur dann sicher nachweisen lassen, wenn sie von unseren IT-Sicherheitsexperten aktiv ausgenutzt bzw. verifiziert werden.

Häufig verbergen sich hinter derartigen IT-Sicherheitslücken weitere schwerwiegendere Sicherheitsprobleme, die erst nach der Ausnutzung identifiziert werden können. Wir empfehlen deshalb, den Testumfang so wenig wie möglich einzuschränken – für einen Angreifer würden derartige Einschränkungen schließlich ebenso wenig gelten.

Unabhängig davon legen wir ein besonderes Augenmerk auf eine systemschonende Testdurchführung und setzen potenziell stabilitätsgefährdende Tests nur nach erfolgter Rücksprache und in enger Abstimmung mit Ihren IT-Verantwortlichen um. Somit garantieren wir jederzeit eine reibungslose und erfolgreiche Testdurchführung.

3 – Die zeitliche Planung eines Penetrationstests

Die Kalkulation des zeitlichen Umfangs basiert auf mehreren Faktoren:

- Anzahl der zu überprüfenden Systeme
- Art der zu überprüfenden Systeme
- Anzahl der Überprüfungsszenarien
- Art und Umfang der gewünschten Ergebnisdokumentation

Als Richtwert für den zeitlichen Vorlauf eines Pentests empfehlen wir ein Zeitfenster von 4 Wochen.

4 – Die drei Phasen eines Penetrationstests

Schritt 1:
Informationssammlung

Recherche in öffentlich verfügbaren Quellen nach DNS-Namen, RIPE-Einträgen, Blacklist-Einträgen, Metadaten-Analysen und Kontaktdaten

Ziel:
Ermittlung des Außenbildes des Unternehmens aus Sicht des Angreifers.

Schritt 2:
Erste Ermittlung von Sicherheitslücken

Ermittlung von Schwachstellen durch automatisiertes Scanning

Ziel:
Weiterführende Identifikation von Sicherheitslücken über erreichbare Dienste, offene Ports, erreichbare Applikationen, bekannte Schwachstellen und Fehlkonfigurationen.

Schritt 3:
Analyse der Sicherheitslücken

Überprüfung durch den Pentester, ob und mit welchem Aufwand die Sicherheitslücken ausnutzbar sind (Exploits).

Ziel:
Risikobewertung des potentiellen Schadens.

II. Die sechs meist gestellten Fragen rund um den Penetrationstest

1 – Weshalb ist die Durchführung von Penetrationstests so wichtig für Unternehmen?

Aktuelle Sicherheitsanalysen zeigen, dass Unternehmen weltweit der permanenten Gefahr unterliegen, Opfer von Cyberangriffen zu werden. Die Zahl bekannter krimineller Angreifergruppen ist im Jahr 2019 weltweit auf über 1800 gestiegen, während je Sicherheitsvorfall ein durchschnittlicher Schaden von 3.92 Millionen USD verursacht wurde.

Die meisten Angriffe wurden dabei von Dritten identifiziert (53%) und blieben bis zum Zeitpunkt der Entdeckung durchschnittlich 141 Tage für das betroffene Unternehmen unerkannt. Gleichzeitig verlieren klassische Abwehrmaßnahmen wie Virenscanner und Firewalls weiter an Wirksamkeit. Dies betrifft alle Nutzer: Private, Unternehmen, Staat und Verwaltung.

Die Mehrzahl der Angriffe auf Unternehmen zielt auf den Diebstahl von geistigem Eigentum (22%) oder die finanzielle Bereicherung durch Erpressung (29%) . Letzteres zeigt sich vor allem in der steigenden kriminellen Energie durch die Platzierung von Erpressungstrojanern.

In der Konsequenz sind die Folgen eines erfolgreichen Cyberangriffes in der Regel immens. Es droht nicht nur ein hoher finanzieller Schaden, auch ein durch Datendiebstahl verursachter Imageverlust kann lang anhaltende negative Konsequenzen für Unternehmen bedeuten.

Im Rahmen eines Penetrationstests decken unsere Pentester die IT-Schwachstellen Ihres Unternehmens auf und liefern Ihnen konkrete Handlungsempfehlungen zur Beseitigung aller Defizite. Die Methoden und Werkzeuge, die sie zur Überprüfung einsetzen, entsprechen denen, die auch Cyberkriminelle nutzen.

Penetrationstests dienen damit auch dem Selbstschutz der Unternehmensverantwortlichen, da sie Unternehmensrisiken, wie z.B. Betriebsausfälle oder Reputationsverluste, minimieren sowie die sensiblen Daten ihres Unternehmens und ihrer Kunden schützen.

2 – Welche Überprüfungsszenarien gibt es bei Penetrationstests?

Infrastrukturprüfung

Untersuchung von Geräten und erreichbaren Diensten auf Infrastrukturebene (z.B. um fehlende Patches, Fehlkonfigurationen, erratbare Anmeldeinformationen und andere bekannte Schwachstellen zu identifizieren). Dies beinhaltet sowohl automatisierte als auch manuelle Testaktivitäten.

Applikationsprüfung

Untersuchung auf Anwendungsebene (z.B. Ermittlung unbekannter Schwachstellen in der Anwendungslogik). Dies schließt den Einsatz von automatisierten Scan-Tools ein, der Fokus liegt hier jedoch auf manuellen Testaktivitäten.

Social Engineering

Identifikation von (nicht-technischen) Sicherheitsrisiken in der Organisation aufgrund des Verhaltens der Mitarbeiter und der Effizienz oder des Fehlens von Prozessen. Dies umfasst Versuche, z.B. über betrügerische Telefonanrufe, Phishing-Mails, Rogue Access Points oder USB-Drops Zugriff auf die IT-Infrastruktur zu erlangen oder z.B. mit gefälschten Identitäten sensible Bereiche von Unternehmensstandorten zu betreten. Social Engineering kann auch mit wirksamem Schadcode kombiniert werden, um das tatsächliche Eindringen in die Zielumgebung zu zeigen und das effektive Risiko für die Organisation auf Basis der Realumgebung zu modellieren.

Wireless

Prüfung der Wireless-Umgebung einer Organisation. Dazu gehört die Analyse der eingesetzten drahtlosen Infrastruktur hinsichtlich kryptographischer Konfiguration, Authentifizierungsmechanismen und allgemeiner Fehlkonfigurationen. Zusätzlich wird eine Standortübersicht der Wireless-Umgebung erstellt, die es erlaubt, die legitime WLAN-Infrastruktur abzubilden und nicht autorisierte Systeme (z.B. Rogue Access Points) zu identifizieren und zu lokalisieren.

Physical

Prüfung des physischen Umfelds der Zielorganisation. Dies beinhaltet die Untersuchung von physischen Zugangskontrollen, wie z.B. Schlüsselkarten-basierte Türsysteme, effektive Trennung und Schutz von sensiblen Bereichen, Isolierung von Netzwerkinfrastrukturkomponenten, Defensivmaßnahmen gegen unautorisierte Geräte (z.B. NAC), etc.

Full Scope Penetration Test

Ein Full Scope Penetration Test umfasst die Zusammenführung aller vorgenannter Testbereiche in einem vollständigen Audit und ermöglicht so eine umfassende Sicht auf das Gesamtunternehmen und alle vorhandenen Risiken.

3 – Welche Verfahren gibt es, um einen Penetrationstest durchzuführen?

Generell wird bei der Durchführung eines Penetrationstests zwischen White Box-, Black Box-, und Grey Box Audit unterschieden, die als Testansatz das Wissensprofil eines Angreifers darstellen.

Im Rahmen des White Box Audits werden unseren verantwortlichen Penetrationstestern alle notwendigen Informationen über die IT-Systeme und internen Strukturen Ihres Unternehmens vor Testbeginn zur Verfügung gestellt. Dies umfasst bei Bedarf auch die Bereitstellung von unterschiedlichen Benutzerzugriffen sowie ggf. Quellcode von zu analysierenden Einzelapplikationen in einer Testumgebung.

Im Gegensatz hierzu liegen beim Black Box Audit kaum Informationen über die zu prüfenden IT-Systeme vor. Analog zum Vorgehen eines echten Angreifers müssen vorab möglichst viele angriffsrelevante Informationen beschafft werden, die eine erfolgreiche Durchführung ermöglichen. Damit simuliert diese Art des Penetrationstests einen möglichen Angriff sehr realitätsnah, führt jedoch unter Umständen zu einer geringeren Abdeckung und Überprüfungstiefe als ein White Box Audit.

Das Grey Box Audit beinhaltet eine Kombination aus Black Box Audit und nachgelagertem White Box Audit. Aus ökonomischer Sicht stellt das Grey Box Verfahren damit im Vergleich zum häufig nachgefragten Black Box Verfahren eine effizientere Vorgehensweise dar.

4 – Welche Penetrationstest-Methode ist für Ihr Unternehmen geeignet?

Je nachdem, welche Zielsetzung Sie mit der Durchführung eines Penetrationstests verfolgen, finden wir gemeinsam mit Ihnen die geeignete Form des Testverfahrens anhand verschiedener Kriterien heraus.

Häufig empfehlen unsere IT-Sicherheitsexperten das White Box Audit, da mit diesem Verfahren eine optimale Abdeckung der zu untersuchenden Systeme gewährleistet wird und somit sehr effektiv relevante Schwachstellen identifiziert werden. Des Weiteren sollte diese Variante generell bei der Prüfung von Einzelanwendungen gewählt werden.

DDoS-Attacke – ja oder nein?

Unseren Pentestern wird häufig die Frage gestellt, ob es sinnvoll ist, einen Distributed Denial of Service-Angriff (DDoS) im Rahmen eines Penetrationstests durchzuführen. Aus Sicht unserer IT-Sicherheitsexperten ist dieses Testverfahren sinnvoll, wenn Sie bereits DDoS-Schutzmechanismen implementiert haben und deren Wirksamkeit überprüfen möchten. Ansonsten raten wir von diesem Testverfahren eher ab, da die zur Verfügung stehende Netzwerkkapazität Ihres Unternehmens komplett ausgelastet würde und technische Beeinträchtigungen die Folge wären.

5 – Ist die Durchführung einer Innentäter-Simulation empfehlenswert?

„Ein interner Penetrationstest gibt mehr Aufschluss über das tatsächliche Sicherheitsniveau eines Unternehmens als zehn externe.“ – Clemens Rambow, Offensive Security Architect bei Allgeier CyRis.

Entgegen der oft vertretenen Meinung, „Angriffe kommen immer von außen, daher müssen die Systeme auch primär von außen abgesichert werden“, bergen die intern erreichbaren IT-Systeme erfahrungsgemäß das deutlich größere Risiko. Typischerweise befinden sich in internen Netzen oft zu wenig wirksame Kontrollmechanismen, nachlässig gewartete oder sogar nicht dokumentierte Systeme und eine riskante Berechtigungsvergabe. Daher ist es einem Angreifer aus dieser Perspektive sehr häufig möglich, in kurzer Zeit die Kontrolle über die gesamte IT-Umgebung zu erlangen. Tatsächlich muss es sich bei einem Innentäter nicht einmal um einen eigenen Mitarbeiter handeln, sondern auch externe Dienstleister oder gekaperte interne PCs können zu Innentäter-Angriffen führen.

Im Rahmen einer Innentäter-Simulation erhalten wir von Ihnen einen repräsentativen Arbeitsplatzrechner inklusive einem Standard-Benutzerzugang. Ausgehend von diesem System versuchen wir, unsere Berechtigungen so weit wie möglich auszuweiten und in andere Netzbereiche vorzudringen – oft mit dem Ergebnis, dass sogar die Kontrolle über vermeintlich isolierte Produktionsnetze möglich ist und keine interne Überwachung Alarm schlägt.

Es bietet sich häufig an, Innentäter-Simulationen mit Aspekten des Social Engineering zu kombinieren, um zusätzlich die Einhaltung von internen Richtlinien (z. B. keine Passwörter auf Post-its, keine vertraulichen Dokumente im Papiermüll, ungesperrte Desktops) oder die Effektivität physischer Schutzmaßnahmen zu prüfen.

6 – Wodurch zeichnet sich der Penetrationstest von Allgeier CyRis im Vergleich zu anderen Dienstleistern aus?

Die Ergebnisse unserer Audits umfassen nicht nur die technische Dokumentation der Schwachstellen und Behebungsmaßnahmen, sondern gehen im Berichtsumfang deutlich über Branchenstandards hinaus. Wir ordnen Befunde unterschiedlichen Schwachstellenkategorien zu und analysieren ihre Verteilung, wodurch wir Rückschlüsse auf deren Ursprung ziehen können.

Auf Basis aller Informationen formulieren wir zusätzlich strategische Maßnahmenempfehlungen mit dem Ziel, das erneute Auftreten ähnlicher Schwachstellen dauerhaft zu verhindern.

Um Ihnen ein plastisches Bild Ihres Sicherheitsniveaus zu liefern, enthält unsere Management Summary:

1. Eine Analyse des Schadpotenzials, welche die konkreten Auswirkungen auf Ihren Geschäftsbetrieb darstellt.
2. Eine Analyse der Angriffswahrscheinlichkeit, bei der wir unter anderem unsere Kenntnisse und Erfahrungen zu potenziellen Tätergruppen einbeziehen. Neben dem Ergebnisbericht liefern wir Ihnen alle Befunde zusätzlich auch in Form einer Aktionsplan-Tabelle, die das Koordinieren und Verfolgen von Behebungsmaßnahmen deutlich erleichtert.

Wir orientieren unsere Testverfahren an etablierten Standards und Security-Forschungsprojekten (z. B. PTES, OWASP) und verfolgen die sich jederzeit ändernde Entwicklung der IT-Sicherheitsforschung stetig. Durch aussagekräftige Zertifizierungen (z. B. OSCP, OSCE, OSWE), regelmäßige Trainings und interne Forschung stellen wir ein ausgezeichnetes Kompetenzniveau unserer Offensive Security Consultants sicher und bauen es fortlaufend aus.

III. Wieviel kostet ein Penetrationstest? Drei Fallbeispiele

Mit der Beauftragung eines Penetrationstests von Allgeier CyRis entscheiden Sie sich dafür, ein optimales Sicherheitsniveau Ihrer Dienste und Systeme sicherzustellen und somit Ihr Unternehmen wirksam vor Schäden, die durch Cyber-Kriminalität verursacht werden, zu schützen.

Aber wie hoch ist die Projektinvestition, die Sie hierfür einplanen müssen?

Mit der Kategorisierung unserer Penetrationstests nach Fallbeispielen geben wir Ihnen eine Übersicht und zugleich auch eine Entscheidungshilfe an die Hand. Wir erläutern Ihnen in Kurzform die am häufigsten von uns durchgeführten Penetrationstests und gehen dabei auf die spezifischen Zielsetzungen, Vorgehensweisen und die zu veranschlagende Investition der einzelnen Untersuchungsmethoden ein.

1 – IT-Schwachstellenanalyse

Projektauftrag

Interner Schwachstellenscan von 50-100 Systemen in bis zu 5 Netzen, Testbereich Infrastruktur

Vorbereitende Tätigkeiten auf Auftraggeberseite

- Zugang zum Netzwerk wird temporär bereitgestellt
- Administrativer Ansprechpartner ist kundenseitig verfügbar / Netzwerkkenntnisse sind vorhanden (ggf. werden Firewall- und Netzwerkanpassungen notwendig)
- Vertragsdokumente müssen vor Beginn der Überprüfung unterzeichnet sein

Tätigkeiten Allgeier CyRis

- Scanning der gewünschten Anzahl von (internen und externen) IP-Adressen auf vorhandene IT-Schwachstellen
- Erstellung eines Ergebnisberichts über alle gefundenen Schwachstellen inklusive Priorisierung dieser nach Gefahrenpotenzial
- Definition einer konkreten Handlungsempfehlung zur Beseitigung jeder identifizierten Schwachstelle
- Übermittlung des Ergebnisreports
- Gemeinsame Besprechung aller Überprüfungsergebnisse

Kundenreferenzen:

Unternehmen der Chemieindustrie
Anzahl der Mitarbeiter: ca. 350

Lottogesellschaft
Anzahl der Mitarbeiter: ca. 120

Projektinvestition:
ca. 3.800 EUR

2 – Black Box Audit

Projektauftrag

IT-Sicherheitsüberprüfung vorab definierter IP-Adressen auf aktuell vorhandene Sicherheitslücken. Den IT Security Consultants liegen kaum Vorkenntnisse über die zu prüfenden Systeme vor.

Vorbereitende Tätigkeiten auf Auftraggeberseite

- Administrativer Ansprechpartner ist kundenseitig verfügbar
- Das Audit muss ggf. beim Hosting-Dienstleister angekündigt werden
- Ggf. Nennung eines Ansprechpartners beim Service Provider (z.B. Webshop, Content Management System etc.)
- Vertragsdokumente müssen vor dem Beginn der Überprüfung unterzeichnet sein

Tätigkeiten Allgeier CyRis

Informationsgewinnung und automatisiertes Scannen sowie Ergebnisauswertung

- Zusammenführung der Informationen und Analyse von Wirkungszusammenhängen (Profiling)
- Validierung der Ergebnisse hinsichtlich False Positives
- Definition der nächsten bzw. „attraktivsten“ Angriffsziele aus Sicht eines Angreifers
- Abstimmung der nächsten Schritte sowie der weiteren Überprüfungsschwerpunkte mit dem Auftraggeber
- Manuelle Analyse der IT-Sicherheitslücken in den identifizierten Applikationen, u.a. Prüfung von unautorisierten Zugriffsmöglichkeiten auf nicht öffentliche Daten, Prüfung der eingesetzten Kommunikations- und Verschlüsselungsverfahren, Überprüfung der Rechte-Verwaltung

Bewertung aller identifizierten Schwachstellen und Ausarbeitung von Handlungsempfehlungen

- Priorisierung der Bedrohungen anhand der Kritikalität
- Erstellung der Ergebnis-Dokumentation mit Management Summary und Aktionsplan
- Vorstellung / Präsentation der Ergebnis-Dokumentation vor Ort
- Erörterung der Handlungsempfehlungen

Optional:

- Retest der gefundenen Schwachstellen
  - Überprüfung der vorab identifizierten Schwachstellen auf deren Behebung
  - Anpassung der Dokumentation inklusive aktualisiertem Behebungsstatus
  - Auf Wunsch: Erstellung eines schriftlichen Testats zum Nachweis des vorhandenen IT-Sicherheitsniveaus
  - Klassifizierung der Ergebnisse anhand Common Vulnerability Scoring System (CVSS 3.0) oder OWASP Top 10

Kundenreferenzen:

Verbraucherportal
Anzahl der Mitarbeiter: ca. 400
Anzahl der zu prüfenden Systeme: 4

Projektinvestition:
ca. 7.100 EUR

Kreditinstitut
Anzahl der Mitarbeiter: ca. 200
Anzahl der zu prüfenden Systeme: 18

Projektinvestition:
ca. 18.200 EUR

3 – White Box Audit

Projektauftrag

IT-Sicherheitsüberprüfung vorab definierter Systeme auf aktuell vorhandene Sicherheitslücken: Den IT Security Consultants werden alle notwendigen Informationen über diese Systeme sowie relevante interne Strukturen des Auftraggebers vor Testbeginn zur Verfügung gestellt.

Vorbereitende Tätigkeiten auf Auftraggeberseite

- Administrativer Ansprechpartner ist kundenseitig verfügbar
- Das Audit muss ggf. beim Hosting-Dienstleister angekündigt werden
- Ggf. Nennung eines Ansprechpartners beim Service Provider (z.B. Webshop, Content Management System etc.)
- Vertragsdokumente müssen vor dem Beginn der Überprüfung unterzeichnet sein

Tätigkeiten Allgeier CyRis

- Übergabe der Informationen für das White Box Audit durch den Auftraggeber, u.a. Netzwerkarchitektur, Betriebssysteme und Applikationen
- Technische Dokumentation der Systeme
- Vorstellung des grundlegenden Funktionsumfangs der Applikation
- Bereitstellung von API-Files (u.a.: swagger, wsda, bdsl) zur Überprüfung der API (wenn vorhanden)
- Ggf. Anmeldung / Freigabe mit dem Hoster abstimmen
- Übergabe von Zugangsdaten (z.B. Demo-Kundenlogin oder Rollenkonzept)
- Prüfung der Informationen und Klärung von Fragen

Informationsgewinnung und automatisiertes Scannen sowie Ergebnisauswertung

- Zusammenführung der Informationen und Analyse von Wirkungszusammenhängen (Profiling)
- Validierung der Ergebnisse hinsichtlich False Positives
- Manuelle Analyse der IT-Sicherheitslücken in den identifizierten Applikationen, u.a. Prüfung von unautorisierten Zugriffsmöglichkeiten auf nicht öffentliche Daten, Prüfung der eingesetzten Kommunikations- und Verschlüsselungsverfahren, Überprüfung der Rechte-Verwaltung

Weiterführende (manuelle) Analyse der Dienste und Systeme inklusive Nutzer-Rollen

Bewertung aller identifizierten Schwachstellen und Ausarbeitung von Handlungsempfehlungen

- Priorisierung der Bedrohungen anhand der Kritikalität
- Erstellung der Ergebnis-Dokumentation mit Management Summary und Aktionsplan
- Vorstellung / Präsentation der Ergebnis-Dokumentation vor Ort
- Erörterung der Handlungsempfehlungen

Optional:

- Retest der gefundenen Schwachstellen
  - Überprüfung der vorab identifizierten Schwachstellen auf deren Behebung
  - Anpassung der Dokumentation inklusive aktualisiertem Behebungsstatus
  - Auf Wunsch: Erstellung eines schriftlichen Testats zum Nachweis des vorhandenen IT-Sicherheitsniveaus
- Klassifizierung der Ergebnisse anhand Common Vulnerability Scoring System (CVSS 3.0) oder OWASP Top 10

Kundenreferenzen:

Verein 1. Fußball-Bundesliga
Anzahl der Mitarbeiter: ca. 300
Anzahl der zu prüfenden Systeme: 5

Rechtsanwaltskanzlei
Anzahl der Mitarbeiter: ca. 450
Anzahl der zu prüfenden Systeme: 9

Projektinvestition:
jeweils ca. 9.800 EUR

Ergänzend zu den oben genannten Penetrationstests optimieren wir die IT-Sicherheit unserer Auftraggeber mit weiteren Überprüfungsmethoden, wie zum Beispiel:

- Social Engineering Audit
- Innentäter-Simulation
- Red Teaming

Wünschen Sie hierzu weiterführende Informationen, laden Sie sich gerne unser Whitepaper zu diesen Überprüfungsmethoden herunter oder kontaktieren Sie uns telefonisch unter +49 (0)421 706 242 1919 oder per E-Mail: info@allgeier-cyris.de

Stand: September 2020

Allgeier CyRis GmbH

+49 (0)421 706 242 1919
info@allgeier-cyris.de
www.allgeier-cyris.de

Hans-Bredow-Straße 60
28307 Bremen