
r tec
cyber security
an accompio company
Sicherheitsanalysen
+ Pentests
Licht ins Dunkel
bringen
© Leonardo Yip | Unsplash

Ad hoc.

Unsere Erfahrung zeigt, dass viele Unternehmen Pentests ad hoc beauftragen und dabei keine langfristige Pentest-Strategie verfolgen. Statt einer zielgerichteten Planung treffen wir häufig auf folgende Szenarien:

- Neue oder geänderte Webanwendungen werden im Rahmen eines Pentests überprüft.
- Am Ende des Jahres ist Budget übrig; nur für vermeintlich kritische Systeme wird ein Pentest beauftragt.
- Ein Audit steht an; für den „Haken“ wird kurzfristig ein Pentest beauftragt.
- Einmal im Jahr werden die kritischsten Anwendungen überprüft.
- In großen zeitlichen Abständen werden umfangreiche Pentest-Projekte durchgeführt.

Probleme und Nachteile

- Ein Pentest ist immer lediglich eine Momentaufnahme. Wenn nicht regelmäßig eine erneute Überprüfung erfolgt, bleiben neue Risiken oder Schwachstellen unerkannt.
- Es handelt sich nicht um eine vollständige Überprüfung. Viele Angriffswege oder Risiken bleiben unerkannt und werden nicht abgesichert.
- Angreifer erreichen ihre Ziele häufig durch die Kombination verschiedener Angriffsvektoren. Werden nur vereinzelt Pentests mit eingeschränktem Scope durchgeführt, bleiben Risiken verborgen.
- Typische Ziele von Angreifern wie zum Beispiel die Rechteerhöhung werden in typischen Pentest-Projekten nicht nachgestellt.
- In typischerweise beauftragten Pentest-Projekten wird die Kompromittierung eines Endgeräts nicht nachgestellt. Dabei reicht bereits eine erfolgreiche Phishing-Mail aus, um ein Endgerät zu kompromittieren.
- Angriffswege über eine mögliche Cloud-Anbindung werden außer Acht gelassen.
- Die Prüfung des Perimeters alleine reicht nicht aus. Angreifer schaffen es nahezu immer, in das interne Netzwerk einzudringen. Ein Pentest des internen Netzwerks, der genau diesen Fall nachstellt, ist somit genauso wichtig wie die Prüfung des Perimeters.

Strategie.

Entwickeln Sie gemeinsam mit uns eine Pentest-Strategie für Ihr Unternehmen. Ziel ist es, mit unterschiedlichen Pentest-Varianten verschiedene Angriffsvektoren zu prüfen sowie deren Kombinationen zu simulieren. Nur so können wir die gesamte Angriffsfläche Ihres Unternehmens sichtbar machen, potenzielle Einfallstore identifizieren und alle notwendigen Handlungsempfehlungen aussprechen. Sie erhalten einen Überblick über die bestehenden Risiken, können Budgetpläne erstellen, verfügbares Budget sinnvoll einsetzen und die Cybersicherheit Ihres Unternehmens kontinuierlich verbessern. Die nachfolgenden Pläne zeigen mögliche Ansätze, die als Basis dienen können und abhängig von Ihren individuellen Anforderungen um weitere Arbeitspakete ergänzt werden sollten.

Plan 1

	ARBEITSPAKETE	ZIELSTELLUNG
Jahr 1	► Externer Pentest ► Interner Pentest	► Erster Überblick über einfach auffindbare und ausnutzbare Schwachstellen des Unternehems
Jahr 2	► Phishing-Kampagne ► Client-Check-up	► Awareness bei Mitarbeitern erhöhen und Risiko bei Social-Engineering-Angriffen ermitteln
Jahr 3	► Webanwendungen	► Tiefgreifende Überprüfung auf Schwachstellen und Fehlkonfigurationen

Plan 2

	ARBEITSPAKETE	ZIELSTELLUNG
Jahr 1	► Externer Pentest ► Interner Pentest ► Phishing-Kampagne ► Client-Check-up	► Fokus auf kritische und von Angreifern zur Rechteerhöhung einfach ausnutzbare Schwachstellen ► Überprüfung und Steigerung der Awareness von Mitarbeitern ► Überprüfung der Härtungsmaßnahmen von Standardendgeräten
Jahr 2	► Webanwendungen	► Tiefgreifende Überprüfung auf Schwachstellen und Fehlkonfigurationen
Jahr 3	► Externer Pentest ► Interner Pentest	► Interne sowie externe Systeme sollten alle zwei Jahre wiederholt getestet werden. So kann die Maßnahmenumsetzung geprüft und eine kontinuierliche Erhöhung der Cybersicherheit vorangetrieben werden.

Strategie.

Plan 3

	ARBEITSPAKETE	ZIELSTELLUNG
Jahr 1	► Externer Pentest ► Interner Pentest ► Phishing-Kampagne ► Client-Check-up ► Webanwendungen	► Fokus auf kritische und einfach ausnutzbare Schwachstellen ► Überprüfung und Steigerung der Awareness von Mitarbeitern ► Überprüfung von Webanwendungen sowie Härtungsmaßnahmen von Standardendgeräten.
Jahr 2	► Red Teaming	► Wiederholte Prüfung interner sowie externer Systeme ► Prüfung der Fähi gkeiten zur Angriffserkennung über das Szenario „Initial Access“
Jahr 3	► Red Teaming ► Webanwendungen	► Wiederholte Analyse von Webanwendungen ► Prüfung der Fähigkeiten zur Angriffserkennung über das Szenario „Assumed Breach“

Plan 1 – geeignet für Unternehmen mit kleinerem Budgetrahmen
Plan 2 - geeignet für Unternehmen mit mittlerem Budgetrahmen
Plan 3 - geeignet für größere Unternehmen mit eigener Angriffserkennung

Tief. Kontrolliert. Erfolgreich.

Wie sicher sind Sie? Mit mehr als 25 Jahren Erfahrung finden wir Schwachstellen, die andere nicht finden. Anschließend können wir Ihnen individuelle Maßnahmenempfehlungen liefern.

- Bei über 90 % der Pentests erlangen wir die volle Kontrolle über das gesamte Unternehmensnetzwerk
- Bei einem Passwort-Audit erhalten wir im Schnitt zwischen 50 und 95 % aller in einem Unternehmen genutzten Klartextpasswörter
- Kürzeste Zeit vom Start bis zur Systemübernahme: 5 Minuten

Pentest Basic

RED TEAM

Wir simulieren einen echten Angriff ohne oder mit einem vordefinierten Umfang und ohne vorherige Information der IT-Abteilungen, sodass wir Ihr Unternehmen aus dem gleichen Blickwinkel sehen wie ein Hacker. Gegenstand der Überprüfung sind die technischen Schutzmaßnahmen für Ihre Systeme und Daten, die laufende Überwachung, Ihre Prozessabläufe bei der Angriffserkennung und die Sensibilität und das Know-how Ihrer Mitarbeiter.

INTERNER PENTEST

Wir nehmen hier die Sicht eines in Ihrem Netzwerk befindlichen Täters ein und prüfen die Sicherheit interner Systeme, Dienste und Applikationen gegenüber Angriffen und nicht regelkonformer Nutzung.

Die Sicherheitsanalysen können für das komplette interne Netz, für bestimmte Anwendungsumgebungen, definierte Benutzerkonten oder auch kritische Anwendungen wie SAP oder Datenbanken durchgeführt werden.

EXTERNER PENTEST

Wir testen die Sicherheit von Netzwerken, Systemen und Applikationen, die aus dem Internet erreichbar sind, aus der Sicht eines externen Angreifers. Dies ist für Sie die unverzichtbare Grundlage einer umfassenden Risikobetrachtung.

CLIENT-CHECK-UP

Anhand eines vom Auftraggeber bereitgestellten repräsentativen Clients (Standard-PC) werden dessen Härtungsmaßnahmen überprüft. Zusätzlich werden Möglichkeiten eines Angreifers mit physikalischem Zugriff auf einen Client-PC untersucht. Ziel ist es, eine Aussage über das Gefährdungspotenzial der Server bei Angriffen und deren mögliche Auswirkung zu erhalten.

PHISHING-KAMPAGNE

Wir definieren zusammen mit Ihnen eine Phishing-Kampagne mit dem Ziel, das Sicherheitsbewusstsein der Mitarbeitenden in Bezug auf gefälschte E-Mails mit präparierten Links oder Anhängen zu prüfen.

SERVER-HÄRTUNG

Anhand eines vom Auftraggeber bereitgestellten repräsentativen Servers werden dessen Härtungsmaßnahmen sowie die Datenbanksicherheit und gegebenenfalls eingerichtete Webserverkonfigurationen überprüft. Ziel ist es, eine Aussage über das Gefährdungspotenzial der Server bei Angriffen und deren mögliche Auswirkung zu erhalten.

ÜBERPRÜFUNG DER AZURE CLOUD

Wir simulieren einen Angriff auf Ihre Azure-Cloud-Umgebung. Ziel des Angriffs ist, die Rechteerhöhung über Azure-Active-Directory-Schwachstellen oder Fehlkonfigurationen der in der Cloud befindlichen Server oder Clients.

WEBANWENDUNGEN

Webapplikationen, Content-Management-Systeme und Portallösungen, auf denen häufig kritische Daten liegen und deren Verfügbarkeit direkte Auswirkungen auf digitale Geschäftsprozesse und -modelle hat, sind oft der verwundbarste Teil der IT-Infrastruktur.

Wir prüfen im Rahmen der Sicherheitsanalyse diese Webapplikationen, Webservices, CMS-Systeme oder Portallösungen wie auch die zugrunde liegende Infrastruktur (Web-, Applikations- oder Datenbankserver) auf Schwachstellen. Ziel ist es, gerade in diesen kritischen Bereichen Risiken zu identifizieren.

Pentest Complete

AWARENESS-VERANSTALTUNG

In Form eines Vortrags mit ergänzendenLive-Hacking-Elementen werden den Teilnehmern praxisnahe Beispiele von Angriffen und deren Auswirkungen nähergebracht. Themen wie Social Engineering, Umgang mit Wechselmedien, Passwortchaos oder Phishing werden in einer Geschichte dargestellt, die den fiktiven Mitarbeiter »Horst« in seinem Arbeitsalltag begleitet. Horst tappt dabei in verschiedene Fallen von Cyberkriminellen, die während des Vortrags interaktiv mit dem Publikum diskutiert werden. Im Anschluss an jedes Thema wird den Teilnehmern das richtige Verhalten in diesen Situationen nähergebracht.

GEBÄUDESICHERHEIT

In diesem Modul prüfen wir Zutrittskontrollmaßnahmen sowie die Wachsamkeit Ihrer Mitarbeiter in Hinblick auf fremde Personen. Dafür versuchen wir in zuvor mit Ihnen definierte Räumlichkeiten einzudringen. Es kommen dabei ausschließlich »weiche« Methoden zum Einsatz, welche zum Beispiel die Ablenkung des Pförtners und den Zutritt durch Tiefgaragen oder Nebeneingänge beinhaltet. Es werden keine Manipulationen an Zutrittskontroll-, Alarm- oder Überwachungsanlagen durchgeführt.

INTERNET OF THINGS

Wir prüfen die eingebettete Firmware auf Verwundbarkeit und geben Ihnen eine Beurteilung des Sicherheitsstatus dieses wichtigsten Bindegliedes zwischen Hard- und Software. Übernimmt ein Angreifer die Kontrolle, sind alle nachgelagerten Schutzmaßnahmen wirkungslos.

NETZWERKSEPARIERUNG

Wir prüfen, wie leicht ein Netzwerkzugang (Ethernet) genutzt werden kann, um am internen Netz teilzunehmen. Insbesondere wird überprüft, ob und welche Maßnahmen ergriffen wurden, um die Teilnahme fremder Systeme am internen Netzwerk zu erschweren. Dabei wird sowohl ein passiver als auch aktiver Angreifer simuliert. Sollten Verfahren wie Network Access Control (NAC) eingesetzt werden, wird versucht, diese zu umgehen.

TERMINAL-SERVER-AUSBRUCH

In diesem Arbeitspaket wird untersucht, inwieweit beschränkte Benutzer aus den vorgesehenen Terminalumgebungen ausbrechen können, um ggf. unbefugt auf Dienste bzw. sensible Daten zuzugreifen.

MOBILE APPS

Durch eine umfassende Analyse von mobilen Apps im Kontext des Betriebssystems erhalten Sie ein Verständnis für Risiken durch mobile Anwendungen des Unternehmens oder Dienst-Smartphones.

ICS/SCADA

Gerade IP-fähige Automaten, Steuer- und Kontrollsysteme (z. B. SCADA/ICS in Energiewirtschaft, Prozesstechnik, Medizin und Handel) sind besonders risikobehaftet und werden in Sicherheitsbetrachtungen häufig nicht mit einbezogen. Wir testen diese auf Zugriffsmöglichkeiten und Sicherheitslücken und zeigen die Schwachstellen in Industrieumgebungen auf, bevor sie durch Angreifer ausgenutzt werden.

WLAN-AUDIT

Wir nehmen eine Sicherheitsprüfung und -bewertung vorhandener WLAN-, Bluetooth- und Funkperipherienetze vor, inklusive einer Ermittlung der Netzabdeckungen. So liefern wir Informationen und die Grundlage für das Verständnis für die Datenübertragungssicherheit in lokalen Funknetzwerken, kabellosen Tastaturen und Mäusen.

STEUERUNGS- UND LEITNETZE

Zur Analyse der Sicherheitsmaßnahmen von Steuerungs- und Leitnetzen führen wir verschiedene Pentest-Szenarien durch (physischer Zutritt, Social Engineering, die Pentests Perimeter und Leitnetz, Kompromittierung Office-Client). Sie erhalten individuelle Maßnahmenempfehlungen zur Absicherung Ihrer Steuerungs- und Leitnetze. Im besten Fall führen wir die Szenarien in einer redundanten Umgebung durch, sodass keine Produktivsysteme gestört werden.

r-tec cyber security
an accompio company

Als Cyber Security Provider mit mehr als 25 Jahren Erfahrung sehen wir Readiness als Kern unserer Leistung: Wir versetzen Unternehmen, Organisationen und Betreiber kritischer Infrastrukturen in die Bereitschaft, Cyberangriffe souverän abwehren zu können.

Dafür konzipieren wir Cyberabwehrstrategien, bieten maßgeschneiderte Cyber Security Services, empfehlen passende Herstellerprodukte und betreiben implementierte Lösungen. Schwerpunkte liegen auf der Vorbeugung, frühzeitigen Erkennung und Abwehr von Cyberangriffen in IT-, OT-, Cloud-, Big-Data- und IoT-Umgebungen.

Unsere Experten greifen dabei auf das Know-how und die Erfahrung aus hunderten Sicherheitsvorfällen pro Jahr zurück. Mit über 90 Mitarbeitern, unserem Security Operations und Cyber Defence Center bieten wir alle wichtigen Ressourcen, Technologien und Services, um unsere Kunden in die nötige Bereitschaft zu versetzen – ready to protect, ready to respond, ready to perform.

Als integraler Bestandteil der accompio Gruppe nimmt r-tec seit August 2024 die führende Rolle für Cyber Security innerhalb der Gruppe ein.

r-tec IT Security GmbH | Hatzfelder Str. 165–167 | 42281 Wuppertal
www.r-tec.net | +49 (0) 202 31767–100