Thinking Objects

Nach Aussage von Bitkom entstehen Unternehmen jedes Jahr 51 Milliarden Euro Schaden durch digitale Wirtschaftsspionage.

Security Audit und Penetrationstest

Transparenz schaffen - Schwachstellen finden - Risiken verringern

Alle Vorteile auf einen Blick

Erkennen von Schwachstellen

Priorisierung von Gefährdungspotenzialen

Aufdecken von Konfigurationsfehlern

Analyse von Web-Anwendungen

Empfehlung konkreter Schutzmaßnahmen

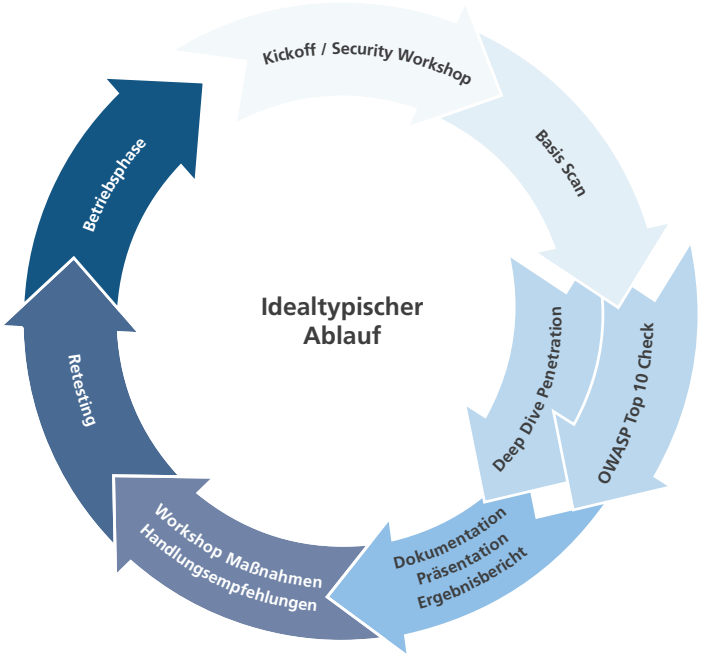
Ableiten eines operativen Maßnahmenplans aus den Ergebnissen

Geringer Aufwand bei vergleichsweise sehr hohem Nutzen

Die Gefahr unerkannter Sicherheitslücken

Erfolgreiche Angriffe auf Portale, Webshops und andere im Internet exponierte IT-Services beeinflussen die Reputation von Unternehmen und können wirtschaftlichen Schaden verursachen. Da sich mit Cyber-Kriminalität heute viel Geld verdienen lässt und Industrie- und Wirtschaftsspionage so allgegenwärtig sind wie noch nie, ist hier für Unternehmen besondere Vorsicht geboten.

Die IT-Services müssen zwar innerhalb der Wertschöpfungskette über das Internet exponiert werden, damit die Zusammenarbeit mit Kunden, Partnern und Lieferanten funktioniert. Jedoch ist es für Unternehmen bisher sehr schwer zu ermitteln, ob diese Dienste auch adäquat geschützt sind. Dies wird in den meisten Fällen durch regelmäßiges Patch-Management, Vertrauen auf eigenes Know-how sowie der Konfiguration von Firewalls und Webservern nach bestem Wissen gelöst. Diese Lösung ist nicht optimal. Vor allem fehlendes Spezialwissen ist eine häufige Ursache für Konfigurationsfehler. Verantwortliche für IT und Sicherheit, aber auch das Management sind gefordert zu agieren. Im Zweifel haften sie für Nachlässigkeit und die daraus resultierenden Konsequenzen.



Wählbare Module

- Kickoff mit Security Workshop
- Basis Scan externer und interner IP-Adressen
- Deep Dive Penetration
- OWASP Top 10 Webserver Analyse
- Ergebnisbericht
- Handlungsempfehlungen inklusive Workshop Maßnahmen
- Retesting
- Betriebsphase

Schwachstellen schnell und zuverlässig aufdecken

Wir bieten als Lösung für dieses Problem die Durchführung eines Penetrationstests inklusive anschließender Maßnahmenempfehlung an. Mithilfe unseres Penetrationstests suchen wir Schwächen, priorisieren die erkannten Risiken und bieten Strategien zur Lösung. Datenlecks, DoS-Attacken und andere Angriffe können somit verhindert werden, bevor sie entstehen. Unser umfangreiches OSCP zertifiziertes Expertenwissen wird dabei in verschiedenen Modulen unterschiedlich genutzt. Das erste Modul beinhaltet eine toolbasierte Schwachstellenanalyse, den sogenannten „Basis Scan". Dieser prüft automatisiert auf Sicherheitslücken. Daran kann mit weiteren Modulen angeknüpft werden. Bei diesen wird Ihre IT-Infrastruktur gezielt von unseren Penetrationstestern angegriffen. Diese vereinbarten Angriffe werden erst von außerhalb und anschließend von innerhalb Ihres Unternehmens durchgeführt. Dies wird je nach Anforderungen um verschiedenen Angriffsszenarien erweitert. Dem Penetrationstester sind dabei die Zugangsdaten und Systeme bekannt. Klassischerweise wird beispielsweise ein Mitarbeiter-PC eingerichtet, von dem aus weitere Sicherheitslücken gesucht werden.

Eine weitere sinnvolle Ergänzung sind Untersuchungen von Webapplikationen, die sich an den OWASP Top 10 orientieren. Hierbei handelt es sich um eine unabhängig erstellte Rangliste der zehn häufigsten Sicherheitsrisiken für Webanwendungen. Alle Module können sowohl im Black-, Grey- als auch White Box-Modus durchgeführt werden.

	BLACK BOX	GREY BOX	WHITE BOX
EXTERN	+	+	+
INTERN	(+)	+	+
SYSTEME BEKANNT	-	+	+
ZUGANGSDATEN BEKANNT	-	-	+

Um eine aussagekräftige und verifizierte Analyse zu gewährleisten, ist es während unseres Penetrationstests nötig, die ermittelten Schwachstellen auszunutzen. Dies geschieht immer in direkter Absprache mit Ihnen, um Ihren produktiven Betrieb nicht oder so wenig wie möglich einzuschränken.

Zu allen Angriffsverfahren und Systemtests erhalten Sie im Anschluss einen ausführlichen technischen Bericht, der ein Management Summary enthält. Wir präsentieren die Ergebnisse zudem gerne vor Ort. So können die Risiken nochmals gemeinsam besprochen, bewertet und Handlungsempfehlungen vorgestellt werden.

Vom Penetrationstest zum Maßnahmenplan

Durch den Penetrationstest können Sie zügig Schwachstellen aus der Sicht eines Angreifers erkennen und anschließend beseitigen. Die vorgeschlagenen Maßnahmen orientieren sich dabei an den vorhandenen technischen und organisatorischen Möglichkeiten.

Das bedeutet im Klartext: Viele der aufgedeckten Schwachstellen können schnell und einfach beseitigt werden, obwohl sie gravierend sind. Für alles Übrige kann direkt ein Maßnahmenplan abgeleitet werden. Dadurch wird das Sicherheitsniveau Ihrer Infrastruktur in kurzer Zeit deutlich gesteigert.

Häufig sind weitere Optimierungspotenziale bereits in den empfohlenen Maßnahmen enthalten. Bei einem Penetrationstest handelt es sich jedoch um eine „Momentaufnahme", daher sind regelmäßige Systemtests, Schwachstellenmanagement und interne IT-Security Workshops hilfreich, um das erreichte Niveau Ihrer Datensicherheit aufrecht zu erhalten.

Thinking Objects GmbH
Lilienthalstraße 2/1
70825 Korntal-Münchingen

+49 711 88770400
info@to.com
www.to.com