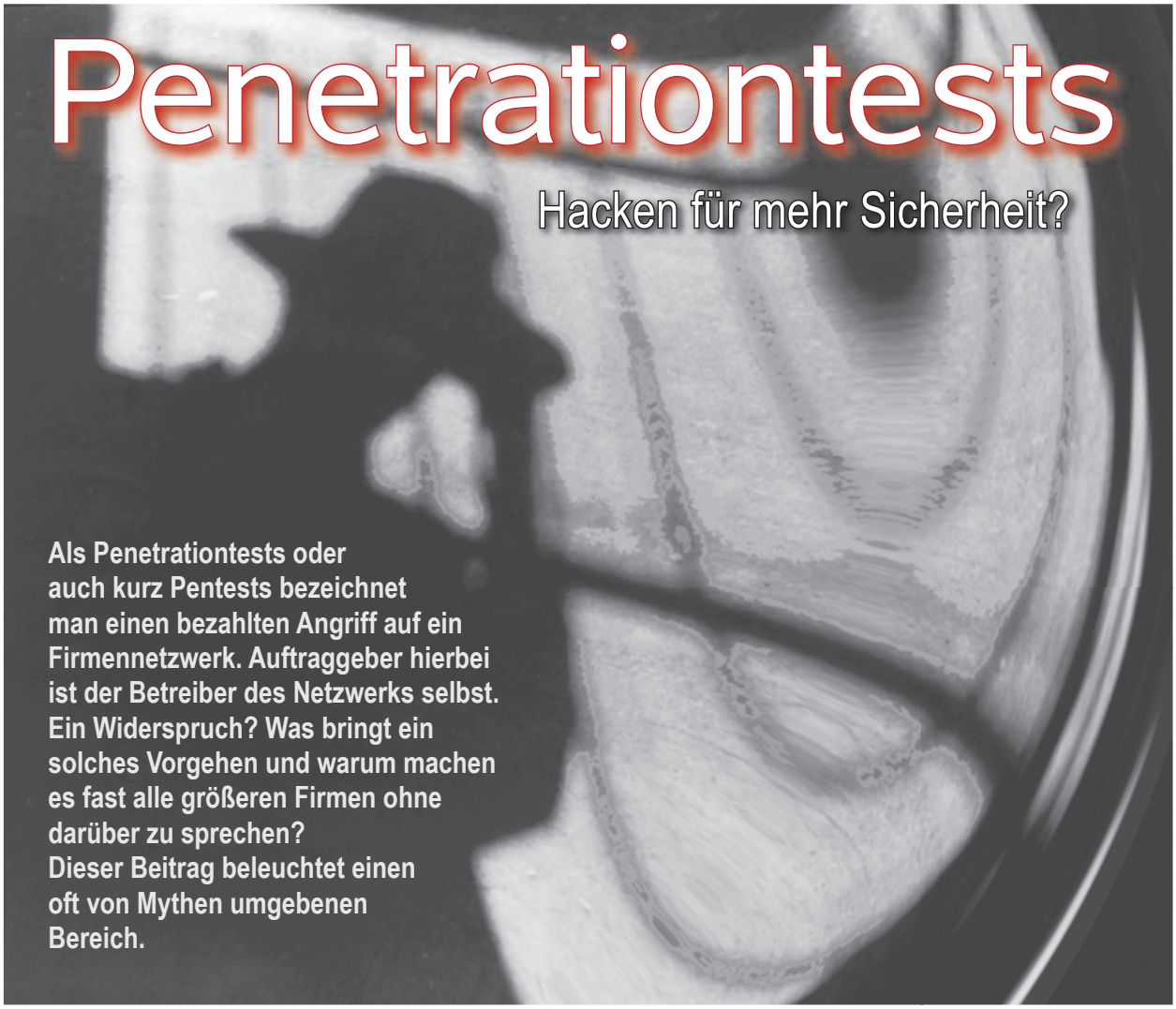
Penetrationtests

Hacken für mehr Sicherheit?



Als Penetrationtests oder auch kurz Pentests bezeichnet man einen bezahlten Angriff auf ein Firmennetzwerk. Auftraggeber hierbei ist der Betreiber des Netzwerks selbst. Ein Widerspruch? Was bringt ein solches Vorgehen und warum machen es fast alle größeren Firmen ohne darüber zu sprechen? Dieser Beitrag beleuchtet einen oft von Mythen umgebenen Bereich.

IT-Sicherheit durch Pentests

Hand aufs Herz, wissen Sie, was genau ein Pentest ist? Nein? Dann stehen Sie nicht alleine da. Selbst manche Kunden, die Pentests beauftragen, haben oft nur ungenaue Vorstellungen, wie ein Pentest funktioniert und warum gerade Attacken auf das eigene Netzwerk das Mittel der Wahl sind, wenn es um IT-Sicherheit geht. Große Unternehmen lassen fast ausnahmslos Pentests durchführen. Auf den folgenden Seiten erfahren Sie, was genau darunter zu verstehen ist.

Ein Pentest ist zunächst einmal eine Sicherheitsüberprüfung in der IT-Welt. Hierbei beauftragt ein Kunde ein Pentestingunternehmen, einen Test aus der Angreiferperspektive durchzuführen und so mögliche Schwachstellen aufzudecken. Angriffsziel ist normalerweise das Firmennetzwerk des Kunden, es kann aber auch ein sicherheitsrelevantes Produkt sein, wie zum Beispiel eine Software, die der Kunde herstellt.

Das entscheidende Merkmal dieser Definition ist die Angreiferperspektive. Ein guter Pentest ist immer sehr praxisnah. Es werden genau die Schwachstellen aufgedeckt, die in der Praxis eine Rolle spielen. Dies funktioniert aber nur, wenn die Tester das Netzwerk mit den Augen eines Angreifers betrachten. Ein Beispiel aus der Praxis soll dies verdeutlichen: Angriffsziel war das Unternehmensnetzwerk eines mittelständischen Unternehmens mit circa 200 Mitarbeitern und mehreren Gebäuden.

Zuerst verschafften sich die Penetrationtester über verschiedene technische Möglichkeiten, etwa über Schwachstellen in der Unternehmenswebseite, Zugriff auf interne Bereiche. Im zweiten Schritt konnten sie recht problemlos, aber profitabel ein unscheinbares Netzwerkkabel auf dem Dach eines der Gebäude angreifen. Dieses versorgte eine Laserstrecke, welche zur Anbindung eines zweiten Firmengebäudes diente. Dieses Kabel befand sich an der Außenseite

und ein Angreifer – und damit auch die Pentester – konnten sich über dieses Kabel direkt mit den internen Bereichen der Firma verbinden. Somit waren dieses Kabel und die unverschlüsselten Daten, die darüber übertragen wurden, als genauso gefährdet einzustufen, wie die anderen Schwachstellen, die ein Eindringen in den internen Bereich ermöglichten. Genau hier zeigt sich der Wert der Angreiferperspektive, die bei Pentests eine große Rolle spielt: Ein echter Angreifer findet solche Schwachstellen, also muss ein Pentester diese ebenfalls finden.

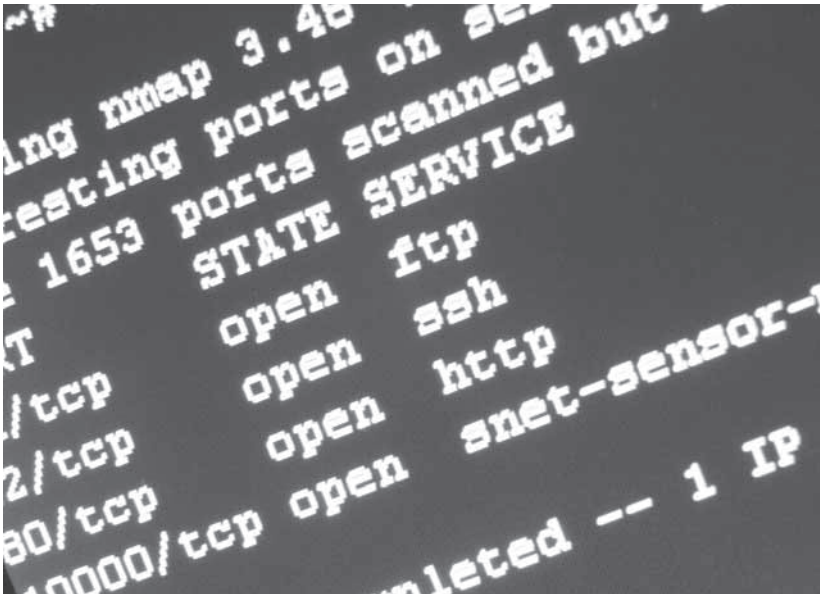
Chronologie eines Pentests

Wie läuft ein Pentest nun ab? Jeder Pentest beginnt noch vor Vertragsabschluss mit einem Vorgespräch, in dem abgeklärt wird, was grundsätzlich getestet werden soll und welche Testmöglichkeiten bestehen. Jedes Netzwerk ist unterschiedlich, und insofern muss zunächst ein sinnvoller Zeitrahmen für den Pentest gefunden werden. Es gibt immer eine Zeitschwelle, unter der ein Test keine sinnvollen Ergebnisse bringen kann, genauso wie es eine obere Grenze gibt, ab der vermutlich keine neuen relevanten Erkenntnisse aus dem Test gezogen werden können, die den Einsatz der Mehrkosten rechtfertigen könnten. Das Vorgespräch dient also dazu, die Kosten und den Nutzen für den Auftraggeber noch vor der eigentlichen Auftragserteilung kalkulierbar zu gestalten. Auch wenn es schwer vorstellbar erscheint: Die Praxis zeigt, dass ein erfahrener Pentester die Zeitdauer relativ gut und genau abschätzen kann.

Nach dem Vorgespräch kommt es zum Vertragsabschluss und der Pentest kann beginnen.

Dieser ist umrankt von Mythen, die aber nicht wirklich zutreffend sind: Ein Pentester wird als professioneller Dienstleister niemals etwas unternehmen, was der Kunde so nicht wünscht oder genehmigt hat. Um auf obiges Beispiel zurückzukommen: Hier sind Mitarbeiter des Kunden mit auf das Dach gestiegen, um die Situation bereits während des Tests beurteilen zu können. Letztendlich lebt ein Pentestingunternehmen von seinem Ruf und entsprechend wird kein zweifelhaftes Pentestingunternehmen von einem größeren Unternehmen einen Auftrag erhalten.

Der eigentliche Test lässt sich grob in vier Phasen einteilen, die aufeinanderaufbauend immer wieder durchlaufen werden:



Der Pentester kennt die Techniken der Hacker

► **Reconnaissance:**
In dieser ersten Phase werden die beauftragten Pentester versuchen, möglichst viele relevante Informationen über den Auftraggeber und dessen Netze aus öffentlichen Quellen zu beschaffen. Oft finden sich bereits hierbei zahlreiche Hinweise, etwa mittels Suchmaschinen. So konnten zum Beispiel in einem Fall schon in dieser Phase komplette Logininformationen für einen internen Datenbankserver gefunden werden, noch bevor überhaupt das betroffene Netzwerk selbst angegriffen wurde. Unmöglich, behaupten viele Firmen. Doch Fakt ist: Informationen, die einmal in Umlauf geraten sind, sind nicht mehr zu kontrollieren. Pentester finden sie, echte Angreifer auch. Und gerade solche Informationen sind riskant: Die angegriffene Firma hat keine Chance einen solchen Angriff vor dem eigentlichen Zugriff auf die Datenbank festzustellen. Doch ist es dann meist schon zu spät.

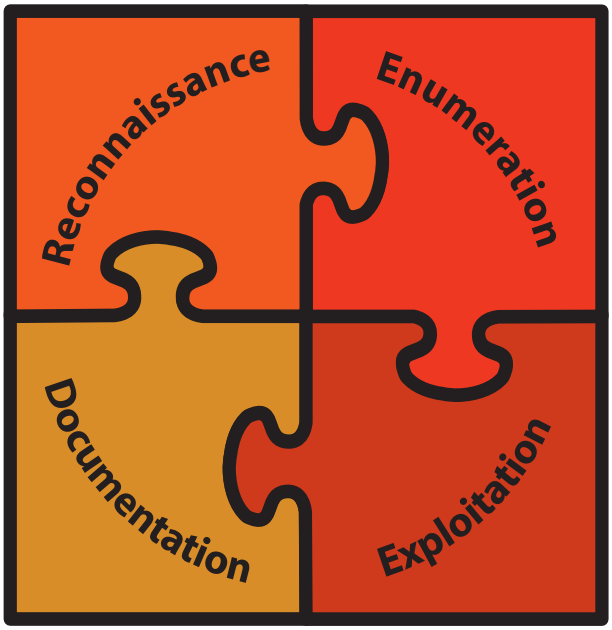
► **Enumeration:**
Hier wird nun direkt mit den Rechnern der Firma kommuniziert. Eine klassische Methode ist unter anderem ein Portscan, der mögliche Dienste identifiziert. Häufig gefundene Dienste sind zum Beispiel Webserver oder Mailserver, die heutzutage viele Unternehmen selbst betreiben. Zu jedem solchen Dienst wird soviel Information wie möglich beschafft. Oft sind die Server mitteilungsfreudig und informieren beispielsweise über genaue Versionsnummern und Betriebssysteme. Interessanterweise unterscheiden sich die gefundenen Informationen oft vom Vorgespräch. Gerne werden Server vergessen oder sind sogar gänzlich unbekannt.

Auch hier wieder ein Beispiel aus der Praxis: Im Rahmen der *Enumeration* wurde ein Server entdeckt, der ein großes Sicherheitsrisiko für den Kunden darstellte, da er offen-

bar seit Jahren(!) nicht mehr auf aktuellem Stand gehalten worden war. Im Abschlussgespräch stellte sich heraus, dass niemand in der Firma von diesem Server wusste und er offensichtlich von einem Administrator gepflegt worden war, der die Firma bereits fünf Jahre zuvor verlassen hatte.

► **Exploitation:**
Hier geht es darum, die vermuteten Schwachstellen aktiv auszunutzen. Natürlich wird vorab entschieden, in wie weit dies für einen Pentest sinnvoll ist. So dürfte es kaum sinnvoll sein, morgens um 11 Uhr die Telefonanlage einer Firma anzugreifen. Dies kann genausogut nach Rücksprache mit dem Auftraggeber am Abend passieren, ohne dass der Test an Aussagekraft verliert, aber auch, ohne dass eventuell 200 Mitarbeiter ohne Telefon in ihrem Büro sitzen. Die verschiedenen Möglichkeiten des *Exploitings* würden den Rahmen dieses Beitrags sprengen: Mit SQL-Injections, Bufferoverflows, Bruteforce-Angriffen sollen nur ein paar von vielen Stichwörtern genannt werden.

► **Documentation:**
Sämtliche Schwachstellen werden während des Tests dokumentiert und in einem Abschlussbericht für den Kunden zusammengefasst. Dieser Abschlussbericht ist in der Regel durchaus umfangreich, da er die Angriffe für die Administratoren nachvollzieh- und wiederholbar darstellt. Zu jeder Schwachstelle gibt es eine Einordnung in Risikoklassen wie auch einen Lösungsvorschlag der Pentester. Neben der sehr umfangreichen technischen Dokumentation wird im Managementkurzbericht auch eine kurze, konzise Zusammenfassung für Entscheider gegeben, anhand der die nächsten Maßnahmen einfach abgestimmt werden können. Im Rahmen einer Abschlusspräsentation stellen die Pentester dann dem Management wie auch dem technischen Personal die Ergebnisse und Lösungen vor und bieten die Möglichkeit, durch eine direkte Diskussion die Ergebnisse des Pentests bestmöglich zu bewerten. So können innerhalb der ersten Tage nach einem Pentest die meisten Sicherheitslücken bereits schnell und unkompliziert geschlossen werden.



Die Phasen eines Pentests greifen nahtlos ineinander über

Im Rahmen des Pentests werden diese Phasen mehrfach durchlaufen. Nach jedem Schritt tiefer in das Netzwerk startet der Pentester wieder von vorne, da gegebenenfalls neue Systeme erreicht werden können. Noch mehr und tiefergehende Informationen zu den Phasen eines Pentests finden sich auf der Homepage von *RedTeam Pentesting (http://www.redteam-pentesting.de/pentest.php)*.

Aufwand und Nutzen

Steht aber der Nutzen eines Pentests wirklich im Verhältnis zum Aufwand, oder wäre es nicht sinnvoller, direkt in neue Hard- und Software für die IT-Sicherheit zu investieren? Wo liegt der besondere Nutzen dieser Investition?

Das Entscheidende ist die Angreiferperspektive: Welchen Sicherheitsgewinn bringt eine neue Anschaffung, wenn es andere bis dahin unbekannte Schwachstellen im Unternehmen gibt, die jedem Angreifer selbst nach der Investition noch Tür und Tor öffnen? Und genau hier liegt der Wert eines Pentests: Ein Pentest ist so praxisnah wie jeder Angreifer auch. Und damit findet er auch genau die Schwachstellen, die ein Angreifer finden würde. Ein Pentest erkennt sehr schnell die relevanten Schwachstellen und dokumentiert diese ausführlich, statt einzelne Symptome zu korrigieren und den Blick für die Gesamtheit zu verlieren.

Ein Pentest hilft somit unnötige Investitionen von vornherein zu vermeiden. Er dient als Entscheidungsgrundlage für weitere Schritte, ist aber nicht zwangsweise mit weiteren Investitionen verbunden.

Oft lässt sich im Gegenteil mit sehr einfachen Mitteln und damit sehr schnell eine Schwachstelle beheben. Und das ist der zweite, entscheidende Vorteil des Pentests, die extrem schnelle Umsetzung und Problembehebung. Es gibt wohl keine andere Methode, in so kurzer Zeit soviel über das eigene Netzwerk zu erfahren. Während andere Maßnahmen noch tief in der Planung sind, ist

Jens Liebchen (RedTeam Pentesting) – Ein gutes Pentestingunternehmen hat mehr als einen erfahrenen Pentester!

der Pentest bereits abgeschlossen. Mit dem Abschlussbericht erhalten die Administratoren etwas in die Hand, mit dem sie sofort nach der Vorstellung die ersten Sicherheitslücken innerhalb von Minuten schließen können. Durch den Umfang der Beschreibungen in einem guten Bericht werden selbst bis dahin unbekannte Schwachstellenarten für die Administratoren greifbar. Praxisrelevantes Wissen fließt direkt – und ohne kostenintensive Schulungen – in die Firma.

Eine weitere grundsätzliche Motivation für Pentests basiert auf indirekten Gründen, klassisch etwa der Werbemöglichkeit mit den Ergebnissen. Gerade bei sicherheitsrelevanten Produkten sind unabhängige externe Expertentests die einzige Möglichkeit, um überzeugend die Sicherheit eines Produktes zu belegen.

Pentests für den Mittelstand?

Interessanterweise hört man selbst in mittelständischen Unternehmen immer wieder das Argument, man sei nicht gefährdet. Doch das ist schlicht und einfach falsch: Ein mittelständischer Unternehmer hat Verantwortung für viele Arbeitsplätze. Eine kurzfristige Auftragsflaute, weil die Konkurrenz seltsamerweise immer das bessere Angebot machen kann, eine Kundendatenbank, die in die falschen Hände fällt, oder auch ein Ausfall der IT zum falschen Zeitpunkt kostet hier schnell viele Jobs. Großunternehmen können eine solche Situation über kurze Zeit kompensieren, Mittelständler oft leider nicht.

Und trotzdem: Die Großen führen meist jährlich Pentests durch - und der Mittelstand? Pentests scheinen hier noch unbekannt zu sein. Stattdessen werden gerne externe Consultants oder andere Dienstleister eingeladen, die dann jeweils hier und da etwas verbessern. Leider meist ohne Blick für das Ganze. Auch hier ein Beispiel aus der Praxis: Nachdem in einem Unternehmen immer wieder Daten entwendet wurden, beauftragte die Geschäftsleitung eine Firma, hierfür Lösungsideen zu entwickeln. Heraus kam eine Verschlüsselungstechnik mit Chipkarten nach aktuellem Stand der Technik, die für alle möglichen Einsatzszenarien genutzt werden konnte. So wurden kritische Daten mithilfe der Karten verschlüsselt abgelegt, der Benutzerlogin funktionierte statt mit Passwörtern nun mit den Karten. Alles hörte sich gut an, bis auffiel, dass sämtliche Daten intern per eMail verschickt wurden und genau hier keinerlei Verschlüsselung genutzt wurde.

Manager und Geschäftsleitung müssen erkennen, dass es keine out-of-the-box Lösung für IT-Sicherheit gibt, auch wenn manche Lösungen dies vorgeben. Ein Pentest bringt Licht in das eigene Netzwerk und hilft, die richtigen Entscheidungen zu treffen. Und ganz nebenbei ist er kostengünstig und bringt oft sogar auf mittelfristige Sicht Einsparpotenzial mit sich.

Gerade bei webbasierten Produkten, wie sie im Moment gerne und überall genutzt werden, sollte ein Pentest vor dem Verkauf eigentlich zum guten Ton gehören. Leicht schleichen sich Fehler ein, die intern schnell übersehen werden. Wird ein solches Produkt beim Kunden dann erfolgreich angegriffen, ist der Schaden meist nicht mehr aufzufangen.

Rechtliche Gründe

Es gibt auch rechtliche Gründe, einen Pentest durchführen zu lassen. So finden sich an vielen Stellen der Gesetzestexte Formulierungen, welche die Durchführung eines Pentests zur Validierung der Vorschriften notwendig erscheinen lassen. Das Handelsgesetzbuch (HGB) schreibt zum Beispiel in den *Grundsätzen ordnungsmäßiger DV-gestützter Buchführungssysteme (GoBS)* ein internes Kontrollsystem (IKS) vor: „Als IKS wird grundsätzlich die Gesamtheit aller aufeinander abgestimmten und miteinander verbundenen Kontrollen, Maßnahmen und Regelungen bezeichnet, die die folgenden Aufgaben haben: Sicherung und Schutz des vorhandenen Vermögens und vorhandener Informationen vor Verlusten aller Art. [...]“ *(Rd-Nr. 4.1 GoBS)*. Andere Textstellen schreiben die Datensicherheit vor: „Die starke Abhängig-

keit der Unternehmung von ihren gespeicherten Informationen macht ein ausgeprägtes Datensicherheitskonzept für das Erfüllen der GoBS unabdingbar. [...]“ *(Rd-Nr. 5.1)*, „Diese Informationen sind gegen Verlust und gegen unberechtigte Veränderung zu schützen. [...]“ *(Rd-Nr. 5.3)* oder „Der Schutz der Informationen gegen unberechtigte Veränderungen ist durch wirksame Zugriffs- bzw. Zugangskontrollen zu gewährleisten. [...]“ *(Rd-Nr. 5.5.1)*. Weitere Stellen finden sich im Datenschutzgesetz. Ein vorhandenes Datensicherheitskonzept kann kaum wirkungsvoller getestet werden, als durch einen Pentest.

Gute Pentests, schlechte Pentests

Auf der Suche nach einem geeigneten Dienstleister findet man leider unter dem Begriff *Pentests* auch immer wieder Unternehmen, die zum Beispiel automatische Scans als Pentests anbieten. Dies wird dem Begriff keinesfalls gerecht. Hinzukommt, dass viele Unternehmen der IT-Branche nebenher „auch Pentests“ anbieten. Entsprechend wurde kürzlich auf einer Konferenz von Pentesting als „Me-Too-Business“ gesprochen. Wie erkenne ich also ein gutes Pentesting-Unternehmen?

Ein gutes Pentesting-Unternehmen hat mehrere angestellte Pentester und nicht nur einen („Das ist unser IT-Security-Spezialist.“). Es führt regelmäßig Pentests durch und ist idealerweise hierauf spezialisiert. Ansonsten besteht schnell die Gefahr, dass der scheinbar günstige Pentest nur die Vorarbeit zum Verkauf anderer Sicherheitsprodukte ist, welche dann die gefundenen Probleme auf „magische“ Weise beheben können. Sehen Sie sich deshalb die Internetseiten des potentiellen Anbieters auf diese Fragen hin an. Werden Pentests dort nur am Rande erwähnt oder ausführlich erläutert? Was verkauft das Unternehmen sonst noch? Auf diese Weise können Sie solche unseriösen Anbieter sehr leicht ausschließen.

Nach dieser Vorauswahl vereinbaren Sie ein Vorgespräch. Ein guter Dienstleister wird Ihnen dies aus den beschriebenen Gründen immer anbieten, und zwar kostenlos und ohne Vertrag. Während des Gesprächs werden Sie feststellen, ob und wieviel Erfahrung der Dienstleister in dem Bereich hat. Lassen Sie sich die vier Phasen genau erläutern und gleichen Sie das Gehörte mit den hier ausgeführten Eckpunkten ab. Fragen Sie nach, wer genau den Pentest durchführt. Lassen Sie sich nicht „weitervermitteln“.

Vorsicht ist außerdem geboten, wenn ein Anbieter einen pauschalen Festpreis für einen individuellen Pentest veranschlagt. Die Kosten eines Pentests sind immer konkret kalkuliert, da sich jedes Netzwerk von einem anderen unterscheidet. Bei einem Festpreisangebot zahlen Sie deshalb entweder wesentlich zu viel oder – was nach Erfahrungen in der Vergangenheit von unseren Kunden oft berichtet wurde – Sie erhalten einen unbrauchbaren Test, der Ihnen nicht wirklich weiterhilft und nur eine Ansammlung von Ergebnissen verschiedener mehr oder weniger automatisch ablaufender Skripte ist.

Fazit

Aktuell erkennen mehr und mehr Unternehmen das Potenzial von Pentests. Pentests sind das Mittel der Wahl, wenn es um IT-Sicherheit geht, weil es die umfassendste, schnellste und mittelfristig kostengünstigste Methode darstellt. Die meisten großen Unternehmen haben dies längst erkannt. Im Mittelstand gibt es zur Zeit noch Nachholbedarf, auch wenn mittlerweile immer mehr Kleinunternehmen Pentests beauftragen. Durch ein kleineres und überschaubareres Angriffsziel, sind die Kosten eines Pentests geringer, wodurch er auch für diese Unternehmen erschwinglich wird. Natürlich führt die wachsende Nachfrage auch dazu, dass schwarze Schafe in den Markt drängen. Aber mit vorgenannter Strategie lassen sich diese leicht entlarven, sofern man nicht geblendet von einem günstigen Preis die Fakten eines Pentests vergisst. Viele Firmen, die zum ersten Mal einen Pentest von einem professionellen Pentestingunternehmen durchführen lassen, sind positiv überrascht, wie viele brauchbare Ergebnisse hierdurch in so kurzer Zeit entstanden sind. Auf Rückfrage geben fast 100 Prozent der Unternehmen an, dass der Pentest sehr hilfreich war und sie auch in Zukunft planen, Pentests durchzuführen.

Jens Liebchen arbeitet als Penetrationtester bei *RedTeam Pentesting*. *RedTeam Pentesting* ist auf die Durchführung von Penetrationtests spezialisiert. Zu den Kunden von RedTeam gehören zahlreiche nationale wie internationale Unternehmen. Die Größe dieser Firmen variiert über die gesamte Bandbreite von kleinen, über mittelständische bis hin zu Großunternehmen.

Jens Liebchen
jens.liebchen@redteam-pentesting.de