



PENETRATIONSTEST


Whitepaper 2021




Inhaltsangabe

Was ist ein Penetrationstest?	2
Was kostet ein Sicherheitsvorfall?	3
Zielgruppe	4
Reifegrad	5
Vertrauen	6
Arten von Penetrationstests	7
Aufbau eines Penetrationstests	8
Ergebnis	9
Metriken und Mehrwerte	10
Penetrationstest Greifbar machen	11
Über die AWARE7	12

Was ist ein Penetrationstest?



Dieses Whitepaper widmet sich der Thematik rund um den Return on Investment (RoI) für Penetrationstests. Dieser ist oft höher als von den verantwortlichen Personen erwartet. Das Ziel eines Penetrationstests ist es technische Schwachstellen in informationsverarbeitenden Systemen zu identifizieren, die Ihre Organisation beeinträchtigen könnten. Dabei können unterschiedliche Szenarien angenommen werden:



Der Angreifer von außen, der missgestimmte Angestellte von innen oder ein staatlich gesponserter Angreifer. All dies sind realistische Bedrohungsszenarien.

Wenn Sie einen Penetrationstest buchen, erfahren Sie und Ihre Organisation eine realitätsnahe Cyberattacke mit dem Ziel sich vor echten Angreifern schützen zu können. Bei der AWARE7 GmbH setzen wir dabei auf unsere Analysten, die mit Hilfe von Analysetools und Angriffsstrategien Ihre Infrastruktur, Software oder Hardware angreifen.

Ziel von Hackerangriffen sind heutzutage nahezu alle Formen von Unternehmen, in allen Arten von Branchen. Das Risiko eines erfolgreichen Angriffs muss gemessen und gesteuert werden. Das Mittel der Wahl ist ein professioneller Penetrationstest.

Was kostet ein Sicherheitsvorfall?

Die Frage, welche Maßnahmen der Informationssicherheit Budget erhalten sollte ist individuell zu beantworten. Ein Penetrationstest kann an mehreren Stellen unterstützen und liefert einen hohen RoI. Durch die Generierung und Ableitung von Metriken aus dem Report können Sie als Informationssicherheitsbeauftragter im nächsten Meeting mit dem höheren Management Mehrwerte generieren.

Ein erfolgreicher Angriff kann verheerende Auswirkungen haben. Auf die Reputation und auch auf die finanzielle Situation. Werden personenbezogene Daten gestohlen, kann dies seit Inkrafttreten der DSGVO bis zu 4% des Jahresumsatzes kosten. Ohne die forensischen Analysen, Reputationsverluste und sonstigen Kosten mit einzurechnen.

Die Frage ist also nicht was ein Penetrationstest kostet, sondern ob Sie es sich leisten können Daten zu verlieren?

Ein Sicherheitstest sollte, unabhängig von der Unternehmensgröße, durch externe Experten durchgeführt werden. Die Frage ist also nicht was ein Penetrationstest kostet, sondern ob Sie es sich leisten können Daten zu verlieren?

Ein Sicherheitstest sollte, unabhängig von der Unternehmensgröße, durch externe Experten durchgeführt werden.



2 Mio. Euro

Durchschnittliche Kosten eines Datenlecks für Organisationen mit weniger als 500 Mitarbeiter:innen

25 T. Euro

Durchschnittliche Kosten für einen Penetrationstest bei Unternehmen mit weniger als 500 Mitarbeiter:innen

Zielgruppe

Häufig wird angenommen, dass Penetrationstests nur durch große Firmen durchgeführt werden müssen. Die Wahrheit ist, dass vermehrt kleine und mittelständische Unternehmen ins Visier der Angreifer gelangen. Forschungen zeigen, dass rund 60% der Angriffe auf KMU ausgerichtet sind. Ein erfolgreicher Angriff kann verheerende Auswirkungen haben. Auf die Reputation und auch auf die finanzielle Situation. Werden personenbezogene Daten gestohlen, kann dies seit Inkrafttreten der DSGVO bis zu 4% des Jahresumsatzes kosten. Ohne die forensischen Analysen, Reputationsverluste und sonstigen Kosten mit einzurechnen.

Die Frage ist also nicht was ein Penetrationstest kostet, sondern ob Sie es sich leisten können Daten zu verlieren?

Ein Sicherheitstest sollte, unabhängig von der Unternehmensgröße, durch externe Experten durchgeführt werden. Diese sind unvoreingenommen und liefern ein realistisches Bild der Bedrohungslage ohne selbst Befangen zu sein.



130 Euro

Kosten für einen Datensatz mit personenbezogenen Daten

Reifegrad

Informationssicherheit ist ein Prozess, der verschiedene Reifegrade erreichen kann. Die Durchführung eines Penetrationstests kann Ihnen helfen den nächsten Reifegrad zu erreichen. Je früher Sie Anfangen, desto besser.

Eine mittelschwere Schwachstelle in einem Produktionssystem zu beheben, ohne das Daten abfließen, kostet laut dem "IBM Cost of a Data Breach Report" circa 7.000 EUR während es circa 70 EUR kostet, wenn Sie im Entwicklungsprozess entdeckt wird. Das Aufspüren von Schwachstellen bevor ein System "Live" geht, ist also ein wichtiger Faktor beim Sparen der Kosten. Ein Penetrationstest kann hier einen entscheidenden Vorteil liefern und helfen.

[Der Verizon Data Breach Investigations Report](#) zeigt genau auf, dass die Gründe für eine Schwachstelle durch einen Penetrationstest gefunden werden können:



45 %

der Lecks durch Hacking

43 %

der Lecks durch Web Anwendungen

70 %

der Lecks durch externe Angreifer

Vertrauen

Wem vertraue ich meine Daten an und wem traue ich zu, einen Penetrationstest durchzuführen?

Es ist unerlässlich zu prüfen, ob die durchführenden Firmen und Personen die nötigen Qualifikationen haben. Dies können Universitätsabschlüsse, Zertifikate oder Referenzprojekte der involvierten Analysten oder der Firma sein. So können Sie sicherstellen, dass Sie qualitativ hochwertige Ergebnisse und optimalen Mehrwert erhalten.

Eine Vertraulichkeitserklärung zwischen Ihnen und dem Anbieter des Penetrationstests sollte unterschrieben werden.

Ein Penetrationstest sollte ähnlich wie ein Finanz-Audit betrachtet werden. Ihr Team verfolgt Ausgaben und Einnahmen täglich. Ein Audit durch eine externe Gruppe stellt sicher, dass die Prozesse Ihres internen Teams ausreichend sind und Ihre Systeme entsprechend geschützt sind, beziehungsweise Sie Bewertungs- und Managementprozesse entsprechend optimieren können.

Arten von Penetrationstests



Whitebox Testing

Alle Informationen über das Ziel werden dem testenden Unternehmen mitgeteilt. Diese Art von Tests bestätigt die Wirksamkeit der internen Schwachstellenbewertung und Managementkontrollen, indem sie die Existenz bekannter Software- Schwachstellen und gängiger Fehlkonfigurationen in den Systemen einer Organisation identifiziert.



Greybox Testing

Zwischen White- und Blackbox Test ist der Greybox-Test angesiedelt. Bei einem Greybox-Test haben wir in der Regel Kenntnisse über die Interna eines Netzwerks, möglicherweise einschließlich der Design- und Architekturdokumentation und eines netzwerkinternen Accounts.



Blackbox Testing

Es werden keine Informationen über die Interna des Zielsystems an die testende Firma weitergegeben. Diese Art von Tests wird aus der externen Perspektive durchgeführt und zielt darauf ab, Wege zu finden, um auf die internen IT-Assets einer Organisation zuzugreifen. Dadurch wird das Risiko, dem Angreifer ausgesetzt sind, die unbekannt oder nicht mit der Zielorganisation verbunden sind, genauer wiedergegeben.

Aufbau eines Penetrationstests

Ein Penetrationstest ist immer ein individuelles Projekt, welches auf unterschiedlichen Ebenen immer wieder abgestimmt werden muss. Es lassen sich allerdings bestimmte Prozessbausteine definieren, die durchlaufen werden. Je nach Art und Umfang des gewählten Test wird mehr oder weniger Zeit in einzelne Bausteine gelegt. Zu Beginn des Projektes erfolgt ein Kick Off Gespräch, bei dem Sie sich mit dem Dienstleister über letzte Details verständigen könntne. Der Test selber läuft dann beim Dienstleister durch einen individuellen Prozess. Am Ende des Projektes steht immer der Bericht, den wir an Sie übermitteln und Ihnen vorstellen.



KICK-OFF

ENUMERATION

EXPLOITATION

REPORTING

RECON

IDENTIFICATION

POST EXPLOITATION

Ergebnis

Der für Sie als Kunden wertschaffende Punkt ist der Bericht, welcher am Ende des Penetrationstests formuliert wird. Ein ordentlich durchgeführter Penetrationstest wird Ihnen einen ausführlichen und übersichtlichen Bericht liefern. Dies ist weit mehr, als Sie durch automatisierte Schwachstellenscans erreichen können, da hier der individuelle Businessimpact für Ihr Unternehmen immer Beachtung findet.

Ein Bericht sollte Ihnen helfen die Risiken zu verstehen, die sich auf Basis von technischen Schwachstellen und der Leichtigkeit der Ausnutzung dieser Schwachstellen ergeben. So sind Sie in der besten Position Schwachstellen nachhaltig zu schließen. Die Bedrohung durch Angreifer wird nicht wieder zurückgehen und ein Penetrationstest gehört heute zum essentiellen Teil einer Informationssicherheitsstrategie. Egal welche Größe Ihr Unternehmen hat.

Metriken und Mehrwerte

Schwachstellendichte

Penetrationstest liefern Schwachstellen. Werden diese überwacht und geht ein Trend nach unten, kann diese Kennzahl eine bessere Kontrolle der Systeme darstellen und der darauf bestehenden Schwachstellen.

Schweregrad

Angreifer werden versuchen nicht nur kritische Schwachstellen auszunutzen, sondern mit der Zeit auch Schwachstellen mit niedrigerem Schweregrad. Eine Verfolgung des Trends für jeden Schweregrad ist für Ihr Systemportfolio möglich mit Hilfe von Penetrationstests.

Verhältnis Offene/Geschlossene Schwachstellen

Wie schnell behebt Ihre Organisation Sicherheitsprobleme? Wo benötigen Sie Schulungsmaßnahmen oder andere Hilfe? Dies können Sie mit dieser Metrik verfolgen.

Personalkosten für die Schließung

Schwachstellen die in der Produktion gefunden werden, sind teurer als solche die bei der Entwicklung gefunden werden. Penetrationstests frühphasig anzusetzen führen zu Kostenersparnisse.

Krisensimulation

Das Penetrationstest-Team kennt Ihre Infrastruktur und Ihre Schwachstellen. Daraus lässt sich eine Krisensimulation beziehungsweise Notfallübung ableiten die individuell auf Ihr Unternehmen zugeschnitten ist. Eine solche Simulation bereitet Sie auf den Ernstfall vor und hilft Ihrem Incident Response-Team bei der Vorbereitung und dadurch werden letztlich Kosten gespart.



62 % der Kosten für einen Vorfall können durch einen funktionierenden Incident Response Plan vermieden werden.

Erhöhung der Resilienz von KMU

Bei KMU nehmen die Vorfälle weiter zu und haben in über der Hälfte der Fälle Auswirkungen auf die finanzielle und reale Existenz von Unternehmen. Ein Penetrationstest kann unterstützen, die Auswirkungen auf KMU zu reduzieren und die reale Gefahr der Insolvenz durch einen Cyberangriff abzuwehren. Bei KMU macht sich auch eine fehlende interne Resilienz bemerkbar, da hier fast jeder zweite Angriff durch interne stattfindet, während es bei großen Organisationen nur 36 % sind.



Jedes zweite KMU erfährt spürbare Auswirkungen auf den Geschäftsbetrieb nach einem Cyberangriff.

Penetrationstests greifbar machen

Ein Penetrationstest ist immer ein individuelles Projekt, welches auf unterschiedlichen Ebenen abgestimmt werden muss. Zwischen dem Informationssicherheitsbeauftragten, dem Sicherheits-Team und dem höheren Management muss der Mehrwert von Penetrationstests kommuniziert und dargestellt werden.

Andererseits ist die technische Beseitigung essenziell, da ungesicherte Applikationen, beispielsweise im Internet, ein Risiko darstellen. Insbesondere mit den empfindlichen Strafen durch die DSGVO.



Ungefähr jeder zweite Angriff erfolgt über ungesicherte Web Applikationen

Sicherheitsbemühungen werden sich auch in anderen Bereichen, beispielsweise dem Kundenvertrauen und der Kundenzufriedenheit widerspiegeln, was wiederum Kaufanreize schafft. Ihre individuellen Metriken aus dem Bericht abzuleiten kann helfen, Sicherheitsprogramme als integralen Prozess im Unternehmen zu festigen. Wir unterstützen Sie gern bei der Erstellung von Metriken und bei der Durchführung von Penetrationstests.

Über die AWARE7

Die AWARE7 GmbH ist ein Cyber Security Unternehmen aus Gelsenkirchen das Technologien und Produkte entwickelt sowie Dienstleistungen anbietet, die zur Förderung, Steigerung und Erhaltung des IT-Sicherheitslevels dienen. Durch die praktische Arbeit und die regelmäßige Veröffentlichung von wissenschaftlichen Artikeln gelingt es uns komplexe Betrugs- und Angriffsmethoden zu erklären und zu entdecken, um Unternehmen und Behörden zu schützen.

IT-Sicherheit funktioniert nur, wenn die Technik sicher und die Menschen sensibilisiert sind. Komplexe Angriffe nutzen menschliche Schwachstellen in Kombination mit technischen Sicherheitslücken aus. Betrachten Sie das IT-Sicherheitsniveau in ihrem Unternehmen ganzheitlich auf menschlicher und technischer Ebene. Wir sind in Sachen Sicherheit ganzheitlich an Ihrer Seite.



Kontakt

AWARE7 GmbH
Munscheidstraße 14
45886 Gelsenkirchen
info@aware7.de

Chris Wojzechowski
Geschäftsführer
+49 209 88306761
chris@aware7.de