Darum ist ein Pentest so wichtig

Als Unternehmen ist eine gut ausgebaute IT-Abteilung unerlässlich, um die ganzen Daten, die wichtig für die Firma sind, zu sammeln und um das firmeneigene Netzwerk am Laufen zu halten. Dieses Netzwerk muss geschützt werden. Eine sinnvolle Maßnahme kann hier ein Pentest sein.

Was ist ein Pentest?

Ein Pentest, auch Penetrationstest genannt, stellt das firmeneigene IT-System auf die Probe. Hierfür wird eine externe Firma beauftragt, die sich genau auf derartige Arbeiten spezialisiert hat.

In der Regel wird im folgenden Ablauf das ganze System einmal gründlich durchgecheckt. Hierbei werden vor allem Fehler gesucht und Sicherheitslücken ausfindig gemacht. Man kann sich einen Pentest als eine Art Simulation eines Angriffs durch Hacker vorstellen.
Das ist jedoch nur eine Art der Herangehensweise, da die Tester häufig auch mit Insiderinformationen ausgestattet werden und vollen Zugang zu allen Systemen erhalten. Diese Variante hat den Vorteil, dass man tiefer ins System abtauchen kann, eine Simulation ist allerdings näher an der Realität.
Penetration, Test um Test und Check um Check machen diese Arbeit aus, die auch von turingsecure zuverlässig ausgeführt wird.

Egal für welche Variante man sich letztlich entscheidet, am Ende geht es an die Auswertung. Alle Sicherheitslücken liegen offen und die Probleme liegen auf der Hand. Doch ein Problem zu kennen, löst es noch nicht.

Das passiert nach dem Pentest

Seriöse, kompetente Firmen und Tester bieten nun ihre Hilfe an. Die Lösung des Problems nimmt meistens nicht viele Ressourcen in Anspruch, da der schwierigste Teil, das Finden der Sicherheitslücken, ja schon überstanden ist.
Die gefundenen Lücken sofort schließen zu lassen, ist unfassbar wichtig, um gegen zukünftige Angriffe durch Hacker gewappnet zu sein - wir erklären warum.

Vorsicht ist besser als Nachsicht

Was alles passieren kann, wenn man als Unternehmen gehackt und lahmgelegt wird, kann man sich als Chef nicht einmal in seinen schlimmsten Alpträumen ausmalen. Kommt die tägliche Arbeit zum Erliegen, da das Netzwerk nicht mehr funktioniert, ist das oftmals noch der bestmögliche Fall, der eintreten könnte.
Gefährlicher wird es hingegen, wenn sensible Daten und Informationen der Firma von den Hackern gestohlen werden. Möglicherweise könnten diese gegen das Unternehmen verwendet werden, Erpressung ist nicht ausgeschlossen. Auch das Weitergeben von innovativen Ideen an die Konkurrenz kann durch einen Datenklau schneller passieren als man gucken kann.

Das klingt ziemlich teuer und das ist es auch, weshalb auch hier gilt, nicht am falschen Ende zu sparen. Ein Pentest ist eine Investition für die eigene Sicherheit. Und selbst wenn ein Pentest keine

Sicherheitslücken findet, was er in der Regel jedoch tut, dann hat sich diese Investition immer noch gelohnt. Vorsicht ist besser als Nachsicht, denn ein Datenklau ist hier um einiges kostspieliger als der Pentest an sich.

Doch darf man sich mit einem Pentest im Gepäck auch nicht unendlich sicher fühlen oder zumindest nicht für eine allzu lange Zeit. Es treten immer wieder neue Sicherheitslücken auf und man kann sich sicher sein, dass diese auch von den Hackern gefunden werden. Eine regelmäßige Überprüfung ist also mehr als angebracht.
Auch sollte man sich nicht wegen eines frisch installierten Systems in allzu großer Sicherheit wiegen. Netzwerke sind komplex und nicht fehlerfrei, unabhängig davon, wie lange oder kurz sie schon auf dem Markt sind.