Wie Hacker Websites ausspionieren – Wissen bringt Sicherheit

Auch ein erfolgreicher Banküberfall setzt ein gewisses Ausspionieren der betroffenen Filiale voraus. Öffnungszeiten, Mitarbeiter, Verantwortlichkeiten, Eingänge, Ausgänge, Fluchtwege, Alarmanlagen und so weiter. Je mehr der Angreifer über das Unternehmen weiß, desto leichter oder wirkungsvoller ist letztlich der Angriff.

Hacker gehen ähnlich vor, um in eine Website einzubrechen. Lesen Sie hier, welche Lücken Sie nutzen.

Vor einem erfolgreichen Hacker-Angriff steht das sogenannte “Footprinting” an. Das bedeutet, Informationen über die Computer-Netzwerkumgebung wie Hostnamen, IP-Adressen, Betriebssysteme oder offene Ports werden systematisch gesammelt. Selbst so etwas gewöhnliches wie eine Stellenausschreibung kann hier nützliche Informationen liefern (“Windows-Administrator mit Oracle-Kenntnissen gesucht”). Oder der freundliche Herr vom Kundenservice beantwortet einige Fragen einfach viel zu ausführlich.

Zu den häufigsten Quellen zur Informationsbeschaffung gehören sowohl Maßnahmen des passiven Ausspionierens, als auch des aktiven Ausspionierens mit Hilfe von Tools:

die Firmenwebsite
die Google-Suche
Forenbeiträge
ausführliche Stellenangebote
die Mitarbeiter
Port-Scanner
DNS-Lookup
der Website-Quelltext
…
Um ein kleinen Überblick der häufigsten Fehler zu bekommen, hat Firebrand Training ein kostenloses PDF-Whitepaper herausgegeben – es enthält auch Tipps, wie Sie sich besser schützen können.