

SA-2T: Internet Risikoanalyse

Was bieten wir im Internet an und wie sicher ist dieses?

Sie geben uns eine oder mehrere IP-Adressen, für die eine Risikoanalyse durchgeführt werden soll. Unsere Sicherheitsexperten finden Ihren Anschluss an das Internet heraus und untersuchen, inwieweit aus dem Internet verschiedene Services erreichbar sind – und möglicherweise ein Risiko darstellen.

Die Untersuchung beginnt mit einer IP-Recherche und der näheren Betrachtung und Auswertung der Einträge im Nameservice. Es folgen Ping- und Traceroute-Scans. Aus diesen Informationen gewinnen unsere Experten ein detailliertes Bild Ihrer Maschinen, die aus dem Internet heraus erreichbar sind.

Nachdem auch TCP- (SYN, ACK, FIN), UDP-Portscans und ICMP-Scans abgeschlossen sind, ist bekannt, welche Services von den untersuchten Systemen angeboten werden. Hieraus liegen in Kombination mit einer TCP-Banner-Recherche aussagekräftige Informationen vor, die eine Beurteilung potenzieller Sicherheitsrisiken ermöglichen.

Auf diese Informationen aufbauend setzen unsere Sicherheitsexperten frei im Internet verfügbare Tools, wie z.B. Nessus, Saint oder Sara, gezielt gegen das gefundene Angebot ein. Auch eigene Tools aus der „kleinen Werkzeugkiste des Hackers“ kommen zum Einsatz. Die viel gefürchteten Denial-of-Service Angriffe (DoS) werden durchgeführt, allerdings in enger Rücksprache mit Ihren Administratoren und außerhalb Ihrer Haupt-Geschäftszeiten. Damit ist das Risiko eines überraschenden und möglicherweise folgenschweren Ausfalls Ihrer wichtigen Systeme auf ein Minimum reduziert.

Neben diesen freien Tools kommen auch neueste kommerzielle, jeweils zu lizenzierende Werkzeuge zum Einsatz. Hierbei handelt es sich um die aktuellsten Versionen der Internet Scanner SafeSuite von ISS, dem CyberCop von NAI oder andere, entsprechend gute Programme. Neben den normalen Untersuchungen der Systeme werden auch spezielle Tests Ihrer Firewall, Ihres Webservers und Ihrer Router vorgenommen.

Sie erhalten von uns abschließend eine Auswertung und Zusammenfassung sämtlicher Ergebnisse. Mit enthalten sind natürlich dedizierte Hinweise auf potenzielle Sicherheitslücken und qualifizierte Tipps zur Behebung der gefundenen Sicherheitsrisiken.

Selbstverständlich werden die im Rahmen dieser Bestandsaufnahme gewonnen Daten von uns vertraulich und nach dem Bundesdatenschutzgesetz behandelt. Nach Abschluss der Arbeiten erhalten Sie alle Rohdaten, sämtliche bei uns angefallenen Daten werden sachgemäß vernichtet.