

SA-6TO: Risikoanalyse technisch und organisatorisch

Was bieten wir im Netzwerk nach außen und innen an und wie sicher sind die von außen und innen erreichbaren Server aufgesetzt? Gibt es organisatorische oder physikalische Mängel? Wie sensibilisiert sind die Benutzer?

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 in den 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.

Neben der Untersuchung aus dem Internet heraus erfolgen diese Tests auch innerhalb Ihres Netzwerkes. Damit erfahren Sie, was Ihre Mitarbeiter, die sich möglicherweise auch als „Power-User“ fühlen, für Möglichkeiten haben. Nachdem auch TCP- (SYN, ACK, FIN), UDP-Portscans und ICMP-Scans aus dem Internet und Intranet abgeschlossen sind, liegen in Kombination mit einer TCP-Banner-Recherche aussagekräftige Informationen vor, die eine Beurteilung potenzieller Sicherheitsrisiken ermöglichen. Auf diese Informationen aufbauend setzen unsere Sicherheitsexperten neueste kommerzielle, jeweils zu lizenzierende Werkzeuge gezielt gegen das gefundene Angebot ein. Bei den Werkzeugen handelt es sich um die aktuellsten Versionen guter Programme. Neben den normalen Untersuchungen der Systeme werden auch spezielle Tests Ihrer Firewall, Ihres Webserver und Ihrer Router vorgenommen. Denial-of-Service Angriffe (DoS) werden durchgeführt, allerdings in enger Rücksprache mit Ihren Administratoren und außerhalb Ihrer Haupt-Geschäftszeiten.

Einzelne Server unter Unix, Linux, Windows NT oder 2000 sowie Ihre Firewall werden direkt an der Konsole von unseren Experten bezüglich ihrer sicheren Konfiguration untersucht. Das gleiche gilt für von Ihnen ausgewählte Arbeitsplätze.

Ihre Security Policy wird von unseren Experten vor Ort bei Ihnen gesichtet und bewertet. Deren Erfahrung und die ersten Ergebnisse der technischen Untersuchungen lässt mögliche Lücken in der Security Policy erkennen und beseitigen. Außerdem erfolgt eine detaillierte Untersuchung der Sicherheitsrichtlinien für Administratoren und Benutzer. Die Einhaltung von Eskalationswegen wird durch unsere Sicherheitsexperten überprüft. Daneben erfolgen Versuche durch unsere Sicherheitsexperten, unberechtigt zu wichtigen Servern vorzudringen. Auch Methoden des Social Engineering kommen zum Einsatz.

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.