

VULNERABILITY ASSESSMENT & PENETRATION TEST

Mit diesen beiden unterschiedlichen Ansätzen bieten wir unseren Kunden die Möglichkeit, einen Überblick über aktuelle Schwachstellen in der bestehenden Infrastruktur zu erlangen und/oder das konkrete Gefahrenpotenzial und die Auswirkungen der Schwachstellen zu bestimmen und zu testen. Basierend auf der Erwartungshaltung des Kunden, der Überprüfungshäufigkeit, der finanziellen Mittel und des erwarteten Nutzens kann entweder eine Variante des jeweiligen Produktes erworben oder eine individuelle Kombination erarbeitet werden.

WAS IST EIN VULNERABILITY ASSESSMENT?

Ein Vulnerability Assessment schafft einen Überblick über aktuelle Systemschwachstellen, welche entweder aus dem internen Netzwerk oder über externe Anbindungen angreifbar sind. Mit einem hohen Grad an Automatisierung liegt der Vorteil dieser Überprüfung an dem umfangreichen Schwachstellenreport mit einer Gefahreneinschätzung und konkreten Handlungsvorschlägen.

WAS IST EIN PENETRATION TEST?

Demgegenüber steht ein Penetration Test, der die Effektivität vorhandener Sicherheitsmaßnahmen (Security Hardware, Software, Prozesse usw.) mithilfe eines realistisch simulierten Angriffs überprüft und die tatsächlichen Auswirkungen von Bedrohungen offenlegt. Mit einem hohen Maß an manueller Tätigkeit eines qualifizierten Engineers fokussiert der Penetration Test ein konkretes Ziel. Der Angriff kann entweder aus dem internen Netzwerk, von außerhalb der Organisation, auf eine bestimmte Web Applikation und/oder die WLAN Infrastruktur durchgeführt werden.

Bisherige Überprüfungen bei Kunden konnten von menschlichen Schwachstellen wie beispielsweise der

leichtsinigigen Umgang mit Zugangsdaten oder öffentlich preisgegebene Informationen bis hin zu hochrisikoreichen Bedrohungen mit kritischem Schaden, welche durch den Einsatz veralteter Protokolle entstanden sind, aufgezeigt werden. Durch die Identifikation derartiger Sicherheitslücken, die Bereitstellung von Handlungsmaßnahmen und die spätere Umsetzung durch den Kunden konnte erheblichen wirtschaftlichen Schäden vorgebeugt und die IT-Sicherheit wiederhergestellt werden.

WARUM NTS DER IDEALE ANSPRECHPARTNER FÜR EINE SICHERHEITSÜBERPRÜFUNG IST?

Weil wir ...

- 1 ... ein maßgeschneidertes und eigenständiges Service bieten
- 2 ... Schwachstellen aus der Sicht des Verteidigers und des Angreifers betrachten können
- 3 ... über langjähriges und fundiertes Know-How im IT-Security-Bereich verfügen
- 4 ... bei der Implementierung der Handlungsvorschläge unterstützen können

MEHR INFORMATIONEN IN EINEM PERSÖNLICHEN GESPRÄCH ERHALTEN.

**RELAX,
WE CARE**

www.nts.eu
office@nts.eu

Stand 01.10.2018 | Informationsklasse: Public

Die NTS Netzwerk Telekom Service AG, mit Hauptsitz in Raaba-Grambach bei Graz, wurde im Jahre 1995 von den Vorständen Alexander Albler und Hermann Koller gegründet. Derzeit sind über 284 MitarbeiterInnen an den Standorten Graz, Klagenfurt, Wien, Linz, Salzburg, Innsbruck, Dornbirn, Friedrichshafen, Rosenheim, Leipzig und Bozen beschäftigt.