NETSEC.CO
THE NETWORK SECURITY COMPANY

Phishing Check

Factsheet

Beschreibung

Die meisten Angriffe auf IT-Systeme von Firmen sind heute sogenannte *inside-out* Attacken. Dabei versucht der Angreifer eine Schadsoftware (einen Trojaner) auf einem Computer innerhalb der Firma zu platzieren. Am einfachsten geht dies mit Unterstützung von Mitarbeitenden. Der Angreifer versucht daher, meist mit Methoden des *Social Engineerings*, Mitarbeitende dazu zu bringen, diesen Trojaner zu installieren.

Die effektivste Methode dabei ist das sogenannte Phishing. Dabei wird versucht, z.B. mittels gefälschter E-Mails die Mitarbeitenden dazu zu bringen, ein Dokument zu öffnen oder einen Link anzuklicken. Im Dokument oder hinter dem Link versteckt sich dann die Schadsoftware. Wird das Dokument geöffnet oder der Link angeklickt, wird der Trojaner unbemerkt auf dem Computer des Opfers installiert. Der Trojaner baut dann eine Verbindung über das Internet zum Angreifer auf und dieser kann den infizierten Computer verwenden, um das Netzwerk auszuspionieren und Daten zu stehlen oder zu manipulieren.

Wozu ein Phishing Check?

Mit einem Phishing Check werden realistische Phishing Angriffe simuliert. Ihre Mitarbeitenden erhalten reale Phishing Mails, welche jedoch keinen Schaden anrichten können.

Ihre Mitarbeitenden werden dadurch für das Thema sensibilisiert und können ihre Verhaltensweise, falls notwendig, anpassen. Ihre IT ist mit einem realen Angriff konfrontiert und kann entsprechend reagieren.

- die simulierten Phishing Angriffe sind auf Ihr Unternehmen zugeschnitten
- Ihre IT-Abteilung wird in der Regel nicht eingeweiht
- es werden verschiedene Methoden angewandt
- Sie können Ihre internen Prozesse überprüfen (reagiert Ihre IT angemessen und schnell genug)

Das erhalten Sie

- Anonyme, mehrstufige Auswertung der Ergebnisse des Checks
- Bericht über mögliche Schwachstellen Ihre Awareness-Strategie

Preise

Pauschalpreis abhängig von der Grösse des Betriebes und der Komplexität des Checks