Solution Overview

Social Engineering mit simulierten Phishing-Mails und Malware-Attacken

Die IT-Security-Strategie eines Unternehmens kann noch so gut sein – wenn Angreifer durch cleveres Social Engineering oder Hacking, also durch «soziale Manipulation» Ihrer Mitarbeiter, Zugang zu Passwörtern und anderen vertraulichen Informationen erhalten, sind die besten technischen Sicherheitslösungen nutzlos.

Eine sinnvolle Abwehrmaßnahme gegen Social Engineering Angriffe ist die Förderung einer positiven Security-Awareness-Kultur in Ihrem Unternehmen. Neben Security-Awareness-Trainings unterstützen verschiedene Angriffssimulationen dabei, die Mitarbeiter für verschiedene Angriffsmuster zu sensibilisieren – zum Beispiel durch professionelle Simulation von E-Mail-Phising- und Malware-Attacken. Im Fokus stehen vor allem Mitarbeiter der Management-Ebene, da diese aufgrund ihrer Führungsposition über mehr sensible Informationen verfügen, welche oft auch noch durch spezielle «Sonderbehandlungen» schlechter geschützt sind.

Social Engineering Service «Management Hack»

Allgemein umfasst das Service-Angebot des «Management Hack» die Überprüfung der IT-Sicherheit (Technische Schwachstellen), sowie die Analyse von Fehlverhalten der Mitarbeiter (Menschliche Schwachstellen). Neben telefonischen Recherchen oder Online-Nachforschungen im Social Media Umfeld (LinkedIn, XING, Facebook) kommen vor allem Social Engineering Techniken wie das Phishing und das personalisierte Spear-Phishing in Kombination mit Malware-Angriffen zum Einsatz.

Eine perfekt gestaltete Phishing-Mail und eine professionell wirkende Phishing Website – mehr benötigen die NTT Security Experten in der Regel nicht, um Ihrem Management innerhalb kürzester Zeit geheime Login-Informationen und andere sensitive Daten zu entlocken, eine «gutartige» Software (Test-Malware) auf dem Business Laptop des Managers zu installieren, oder sogar die vollständige Kontrolle des Gerätes zu übernehmen.

Simulation einer Phising-Attacke

- Entwicklung einer Phishing-Website als exakte Nachbildung einer bestehenden Kunden-Website
- Gestaltung einer professionellen Business E-Mail, die den Leser direkt zur Phishing-Website führt
- Versand der Phishing-E-Mail an eine zuvor definierte Mitarbeiter- bzw. Management-Gruppe oder einzelne Zielpersonen
- Abfangen geheimer Login-Daten oder anderer geschäftskritischer Informationen
- Anonymisierte Ergebnisse, Reporting angereichert mit Statistiken

Simulation einer Malware-Attacke

- Entwicklung einer «gutartigen» Software (Test-Malware)
- Gestaltung einer professionellen Business E-Mail mit enthaltener Test-Malware oder mit Link zur Test-Malware
- Versand der Phishing-E-Mail an eine zuvor definierte Mitarbeiter- bzw. Management-Gruppe oder einzelne Zielpersonen
- Reports aus installierter Test-Malware mit grundlegenden Systeminformationen (keine Ausführung von tatsächlich schadhaften Aktionen auf dem Kundensystem, auf Wunsch Übernahme der Kontrolle des Mitarbeiter PCs)
- Anonymisierte Ergebnisse, Reporting angereichert mit Statistiken

Voraussetzungen für «Management Hack»

- NTT Security stellt die Ergebnisse der simulierten Attacke ausschließlich anonymisiert zur Verfügung. Die Identifikation von Personen oder Personengruppen und Rückschlüsse auf diese sind ausgeschlossen. Auf Wunsch und mit schriftlicher Genehmigung werden die Ergebnisse auch nicht-anonymisiert bereitgestellt.
- Der Kunde autorisiert NTT Security, die Sicherheitsmaßnahmen des Unternehmens mit Hilfe von Phishing-E-Mails, simulierter Malware und anderen Social Engineering Aktionen zu umgehen.
- NTT Security trifft angemessene Vorsichtsmaßnahmen zur Vermeidung etwaiger Service-, System- oder Netzwerkunterbrüche und -ausfälle während und aufgrund der Simulation der Attacke. Aufgrund der Art der Prüftätigkeit kann eine Störung bzw. ein Ausfall von Netzwerkdiensten oder Systemen nie vollständig ausgeschlossen werden. NTT Security übernimmt keine Haftung für Ausfälle und Störungen im Rahmen dieser Tätigkeiten

Über NTT Security

NTT Security ist das auf Sicherheit spezialisierte Unternehmen und «Security Center of Excellence» der NTT Group. Mit «Embedded Security» ermöglicht NTT Security den NTT-Group-Unternehmen (NTT Communications, NTT DATA und Dimension Data) die Bereitstellung zuverlässiger Business-Lösungen für Kundenanforderungen in der digitalen Transformation. NTT Security verfügt über 10 SOCs, sieben Zentren für Forschung und Entwicklung sowie mehr als 1.500 Sicherheitsexperten und behandelt jährlich Hunderttausende Sicherheitsvorfälle auf sechs Kontinenten.

NTT Security sichert eine effiziente Ressourcennutzung, indem den Unternehmen der NTT Group der richtige Mix an ganzheitlichen Managed Security Services, Security Consulting Services und Security-Technologie zur Verfügung gestellt wird – unter optimaler Kombination von lokalen und globalen Ressourcen. NTT Security ist Teil der NTT Group (Nippon Telegraph and Telephone Corporation), einem der größten IKT-Unternehmen weltweit. Weitere Informationen über NTT Security finden sich auf: **www.nttsecurity.com**.

Über die NTT Group in Deutschland

Zur NTT Group in Deutschland gehören neben NTT Security die Unternehmen Arkadin, Dimension Data, e-shelter, itelligence, NTT Communications und NTT DATA. In Deutschland beschäftigt die NTT Group rund 5.300 Mitarbeiter. Der Umsatz liegt bei über 1,2 Milliarden Euro. Weitere Informationen zur globalen NTT Group finden sich unter **www.ntt-global.com**.

Unsere Security Services können über diese NTT-Group-Unternehmen bezogen werden:

www.eu.ntt.com, www.nttdata.com, www.dimensiondata.com.