Penetrationstests und simulierte Social Engineering-Angriffe Pro und Contra

Das Testen der Aufmerksamkeit von Mitarbeitern und Dienstleistern gehört zu den Standardwerkzeugen von Sicherheitsorganen in Unternehmen.
Beim Thema Informationsschutz jedoch sind Penetrationstests und simulierte Social Engineering Angriffe sehr mit Vorsicht zu betrachten!

Zu schnell können sie das Auftrag gebende Management gefährden!

Abgesehen davon behindern sie anschließende Awareness-Maßnahmen!
Testangriffe über IT (z.B. via anonym registrierende Phishing Mails) lassen sich gegenüber Mitarbeitern und Betriebsrat noch relativ leicht begründen.
Bei umfangreichen Social Engineering Testangriffen jedoch werden Mitarbeiter mit Methoden getäuscht, die für Ungeschulte nur sehr schwierig zu durchschauen sind!

- Vorbereitende Aktivitäten schließen das Ausspionieren der Zielpersonen mit ein.
- Angreifer stehlen / kopieren im Vorfeld echte Ausweise und Zugangsdokumente.
- Uniformen / Ausweise von Dienstleistern werden kopiert eingesetzt.
- Schwierig zu durchschauende "Man-In-The-Middle-Methoden" werden eingesetzt.
- Bestehende Lücken in Arbeitsprozessen werden genutzt, wobei die Prozesse selbst von angegriffenen Protagonisten durchaus richtig(!) verwendet werden.

Da Ergebnisse und Analysen dieser Tests irgendwann / irgendwem immer offen gelegt werden müssen (z,B dem Betriebsrat), führt dies erfahrungsgemäß bei Mitarbeitern zu Frust und bei allen anderen Involvierten zu massivem Ärger!

WICHTIG:

Vier zusätzliche, selten beachtete Punkte bringen Testprojekte in Gefahr:

1. Betriebsräte lehnen simulierte Social Engineering Angriffe erfahrungsgemäß fast immer ab und bauen gleichzeitig massive Widerstände gegen Sicherheit auf.
   Auch hierdurch werden nachfolgende Awareness-Projekte erheblich behindert.
2. Vorab informierte, zustimmende Betriebsräte stellen sehr oft eine nicht ganz zu schließende Informationslücke dar. Entsprechend vorgewarnt sind eventuell betroffene Mitarbeiter, was Tests ad absurdum führt.
3. FM-nospy kennt mehrere Fälle, in denen nicht informierte Betriebsräte nach Offenlegung von Testergebnissen die Ablösung der Auftraggeber (Geschäftsleitung) erreichten.
4. Die Tester sind danach im geprüften Unternehmen fast immer "verbrannt" und können kaum mehr zu motivierenden(!) Awareness-Schulungen bei den, vorher getäuschten Personen eingesetzt werden.

FM-nospy empfiehlt aus Erfahrung folgende Lösungen/Vorgehensweisen:
→ 2

FM-nospy empfiehlt aus Erfahrung folgende Lösungen/Vorgehensweisen:

Die nachgenannten Wege liefern verwert- und präsentierbare Ergebnisse, OHNE dass Personen vorgeführt und Betriebsräte verärgert werden.

Ein erfreulicher Nebenaspekt:
Diese Vorgehensweise ist aufgrund der deutlich geringeren Vorbereitungsarbeiten **deutlich preiswerter** als ein, durch professionell gestaltetes Social-Engineering vorbereiteter Test.

- Einführung des Betriebsrates in das Thema und den geplanten Versuch
  Z.B. im Rahmen eines kleinen Vortrags mit anschließender Besprechung.
  Ziel: Offizielle Zustimmung des BR.

- In zeitlich deutlichem Abstand *(um ungewünschte Flüsterwarnungen durch BR und andere zu behindern)*:

  > Mehrfache semi-legimitierte Inhouse-Begehungen durch offen agierende, jedoch mit falschen Identitäten ausgestattete Tester.

  > Dabei auch Versuch der Penetration durch offizielle und inoffizielle Eingänge.

  > Testmails mit anonym registrierenden Phishing-Links

- NICHT personenbezogene, fair gestaltete Ergebnispräsentation aller gefundenen Schwachstellen.

- Gemeinsames Erarbeiten eines Awareness-Konzeptes

- Erstpräsentation vor dem Betriebsrat *(Ergebnisse + geplante Awarenessmaßnahmen)*

- Faire Rückmeldung an die Mitarbeiter, verbunden mit zielgruppenspezifischen, motivierenden(!) Schulungen.

- Beteiligung aller Mitarbeiter an nachhaltig wirkenden Folgemaßnahmen.

Die Teams von **FM-nøspy** *sind KEINE "klassischen Sicherheitsexperten", sondern international erfahrene Kommunikationsprofis. Sie untersuchen mit den Augen eines angreifenden Social Engineers, beraten mit jahrzehntelanger Kompetenz in allen Aspekten der Informationsspionage und sind damit eine wichtige Ergänzung für vorhandenes Sicherheitswissen.*

Bitte sprechen Sie mit uns, BEVOR Ihr Unternehmen zu den Opfern gehört!