Social Engineering

eine erste Gefährdungsanalyse

Die meisten Menschen unterschätzen die Gefahr von “SE-Angriffen“, weil Sie potentielle Ziele im Unternehmen nicht klar und sofort erkennen können. Dabei reicht es manchmal schon, “mit den Augen eines Spions“ von außen auf das eigene Unternehmen zu blicken.

Die nachfolgende kurze Checkliste (mit 10 Fragen) hilft Ihnen bei einer ersten Analyse.

1. Existieren Unternehmen / Länder / Behörden / Interessensgruppen, welche an dem, in meinem Unternehmen oder meiner persönlichen Umgebung vorhandenen Wissen, an schriftlichen Informationen dazu oder an Gegenständen interessiert sein könnten?

2. Gibt es in meinem Unternehmen Wissen, Zahlen, Daten und Fakten, die ihm gegenüber Mitbewerbern Vorsprung oder Wettbewerbsvorteil verschaffen?

3. Gibt es in meinem Unternehmen wertvolles “Insel-Wissen“? Eigene Entwicklungen, technische Raffinessen, Formeln, Preiskalkulationen, geplante Patente, vertrauliche Strategien und Verhandlungsprotokolle, deren Verlust oder Bekanntwerden das Unternehmen in erstzunehmende Schwierigkeiten bringen könnte?

4. Befinden sich in meinem Unternehmen Gegenstände (z.B. teure Apparate, Waren oder Rohmaterial), die zu entwenden entweder finanziell oder wegen eines Wettbewerbs-vorteils von Interesse wäre?

5. Ist mein Unternehmen als externer Dienstleister oder Zulieferer für andere Unternehmen aktiv, die ihrerseits wahrscheinlich über wichtiges Inselwissen oder über wertvolles Material (Produkte, KnowHow etc.) verfügen?

6. Agieren in meinem Unternehmen externe Zulieferer oder Dienstleister, deren Mitarbeiter-Loyalität ich nur schwer einschätzen kann? (z.B. IT-Service)

7. Ist mein Unternehmen durch emotional wirkende Faktoren (z.B. Restrukturierung, Entlassungen, Wechsel von Rahmenbedingungen) belastet, die bei Mitarbeitern Frust, Wut, Resignation oder Revanchegefühle hervorrufen könnten?

8. Sind für mein Unternehmen Mitarbeiter öfter auf Reisen, die wertvolles Material oder wichtige Informationen mit sich führen? Z.B. auf Tagungen, Messen oder Kongressen?

9. Existieren im Unternehmensumfeld Personen, deren Verhalten oder Neigungen zu Nötigung oder Erpressung eingesetzt werden könnten?

10. Pflegen viele meiner Mitarbeiter intensive Präsenz in Social Media oder haben viele eine hohe Affinität zu immer neuen Kommunikationstechnologien?

11. Wurden die Mitarbeiter in meinem Unternehmen in den letzten 12 Monaten ernsthaft und im Rahmen eines zielgruppengerechten Seminars über die Gefahren und Techniken des Social Engineering, sowie über Abwehrtechniken informiert?

Wenn Sie auch nur 20% der oben gestellten Fragen mit „ja“ beantworten müssten, sollten Sie umgehend mit uns Kontakt aufnehmen … info@fm-nospy.com