# Regeln für das Social Engineering - das „Sicherheitsrisiko Mensch“ reduzieren

Namhaften Unternehmen, von denen zu vermuten ist, dass Datensicherheit fester Bestandteil ihrer Wertschöpfungskette ist, sind bekanntlich reihenweise sensible und personenbezogene Daten gestohlen worden. Gestohlen von zugriffsberechtigten Mitarbeitern oder von Personen, die sich Zugang zu den Daten verschafften. Die Täter konnten offensichtlich mühelos alle Sicherheitsvorkehrungen umgehen. Egal ob Wirtschaftskriminalität, Industriespionage, Wirtschaftsspionage oder ganz einfach nur der Wunsch einem Unternehmen zu schaden - mit geringem Aufwand kann ein immenser Schaden entstehen. Das „Sicherheitsrisiko Mensch“ wird viel zu oft unterschätzt.

**10 wichtige Regeln können das Risiko minimieren.**

## 1. Das „Risiko Mensch“ konsequent einbeziehen

Das hohe Risikopotenzial „Insiderkriminalität“ muss berücksichtigt werden. Dazu gehören alle internen und externen Mitarbeiter und Dienstleister mit risikobehafteten Autorisierungen und Privilegien (Programmierer, Security- und Server-Administratoren, Systemverwalter, Operateure, Forscher, Entwickler, Geheimnisträger, Trainees usw.). Nicht zu vergessen sind Personengruppen, die nur indirekt mit sensiblen Daten in Verbindung gebracht werden, aber denen aber ein Zugriff auf Datenträger oder Dokumente möglich ist. Dazu gehören Reinigungskräfte, Mitarbeiter von Fremdfirmen für Instandhaltung und Service, Trainees usw.

## 2. Durch ungetrübten Blick Risikoverzerrungen ausschließen

Befindlichkeiten und Voreingenommenheit müssen ausgeschlossen werden. Der ungetrübte Blick, besonders der eines externen Betrachters, garantiert eine unvoreingenommene, neutrale und ganzheitliche Analyse. So können Bedrohungsbild, Schwachstellen und Risikopotenzial konsequent identifiziert werden. Die darauf abgestimmten Sicherheitsmaßnahmen können unbelastet entwickelt und umgesetzt werden.

## 3. Risikopotenzial nach Rollen, Tätigkeiten und Berechtigungen bewerten

Das Risiko- und Gefahrenpotenzial aller betroffenen Personen - bezogen auf Tätigkeiten, Rollen und Berechtigung - muss identifiziert und realistisch bewertet werden. Jede Überbewertung bedeutet Kosten und Aufwand. Jede Unterbewertung bedeutet vermeidbares Restrisiko.

## 4. Das Risiko auf möglichst wenig Personen konzentrieren

Tätigkeiten und damit verbundene Rollen und Berechtigungen so weit wie möglich einschränken und auf möglichst wenig Personen konzentrieren. Die Machtfülle der Personen - gerade bei langjährigen internen und externen Mitarbeitern - richtig bewerten und einstufen. Externe Mitarbeiter besonders kritisch betrachten.

## 5. Die Zuverlässigkeit der Personen konsequent prüfen

Alle Möglichkeiten einer Zuverlässigkeitsprüfung müssen anwendet werden. Bezogen auf Unternehmen mit entsprechendem Schutzbedarf ist eine Zuverlässigkeitsprüfung analog zur Überprüfungstiefe gemäß Luftsicherheitsgesetz LuftSiG, §7 oder zu den Sicherheitsüberprüfungen des Bundes gemäß Sicherheitsüberprüfungsgesetz SÜG, § 9 (Ü2) oder §10 (Ü3) denkbar (Anmerkung: Jeder Mitwirkende am Bau einer Justizvollzugsanstalt muss eine Sicherheitsüberprüfung gemäß SÜG durchlaufen). Da aber für die Privatwirtschaft eine gesetzliche Grundlage für derartige Überprüfungen derzeit noch fehlt, sollte sich die Zuverlässigkeitsüberprüfung zumindest an den dort definierten Prüfkriterien orientieren und durch entsprechende Experten durchgeführt werden.

(Zitat Dr. Stephan Fedtke (Quelle: kes, Ausgabe 12/2010 – Epische Macht): „Ohne Zweifel bestreitet der Mensch in der IT eine Doppelrolle. Er ist elementarer Erfolgsfaktor und höchstes Risiko zugleich. Bei solchen Mitarbeitern liegt eine exzessiv nachteilige und einseitige Risiko-Charakteristik vor. Diese ergibt sich aus dem Verhältnis der Höhe des potenziell angerichteten Schadens (Mio. Euro) zur Realisierungsdauer (ggf. nur Sekundenbruchteile“)

## 6. Arbeitsplätze in Sicherheitszonen konzentrieren

Auch wenn das „Risiko Mensch“ durch qualifizierte Zuverlässigkeits- oder Sicherheitsüberprüfungen minimiert wird, bleibt immer noch ein erhebliches Restrisiko. Entsprechend dem Motto „Vertrauen ist gut, Kontrolle ist besser“ sollten die Personen - nach Rollen und Berechtigungen geordnet - in besonderen Sicherheitszonen zusammengefasst werden. Konsequente Kontrollmaßnahmen können sich dann auf einen oder mehrere kleine Sicherheitszonen konzentrieren und mit geringstem Aufwand umgesetzt werden.

## 7. Sicherungslinien konsequent überwachen

Zu- und Abgänge zu den Sicherheitszonen sollten - auch wenn längere Wege oder Unbequemlichkeiten entstehen - auf ein Minimum reduziert, aber dafür konsequent geregelt und überwacht werden. Sicherheitsschleusen, Personenvereinzelung, elektronische Zu- und Abgangskontrolle in Kombination mit Biometrie und Türzustandsüberwachung, Video-

überwachung, Einbruchmeldetechnik usw. sind natürlich obligatorisch. Die Sicherungslinien müssen klar und deutlich signalisieren: Hier beginnt ein besonderer Sicherheitsbereich, hier gelten besondere Sicherheitsmaßstäbe und Sicherheitsmaßnahmen.

## 8. Das Mitführen unerwünschte Gegenstände verhindern

Es muss eindeutig geregelt werden, welche Gegenstände beim Zugang oder Abgang mitgeführt werden dürfen. Die durchaus unpopuläre Maßnahme sollte alle speicher- und kommunikationsfähigen Geräte mit Internetzugang einbeziehen und sich derzeit an der Größe der USB-Sticks orientieren. An Handgepäck- und Personenkontrollen führt kein Weg vorbei. Es muss individuell entschieden werden, ob ständig oder unregelmäßig kontrolliert wird. Der Fokus der Kontrollen muss auf den Abgang gelegt werden. Ein Umgehen der Kontrollstellen muss zwingend vermieden werden. Ergänzende Maßnahmen innerhalb der Sicherheitszonen sind obligatorisch. Dazu gehören z. B.: Clean Desk, Aufsicht von Reinigungs- und Instandhaltungspersonal, besondere Kontrolle der externer Mitarbeiter.

## 9. Ständige Kontrollen, Revisionen und Optimierungen durchführen

Das in der IT übliche User-Monitoring ist dem Risikopotenzial entsprechend anzupassen, zu verschärfen oder überhaupt einzurichten. Dabei darf nicht vergessen werden, dass der fachlich versierte Insider schnell Sicherheitslücken erkennt und im Fall vorsätzlicher Handlungen auch erfolgsversprechende Möglichkeiten entwickelt, diese zu umgehen. Getreu dem Motto von Curt Emmerich, deutscher Arzt und Schriftsteller **„Ich war mir meiner Sache so sicher und gerade diese Sicherheit war es, der alle Zweifel entsprangen“**, sind alle Sicherheitsmaßnahmen einer ständigen Revision, möglichst durch neutrale Externe, zu unterwerfen und entsprechend zu optimieren.

## 10. Vertrauen und Mitwirkung fördern

Werden Sicherheitsmaßnahmen klar begründet und kommuniziert, werden sie auch als erforderlich wahrgenommen. Durch die frühzeitige Einbeziehung der betroffenen Personen und Personalvertretungen kann das entstehende Konfliktpotenzial deutlich reduziert und Investitionssicherheit geschaffen werden. Regelmäßige Informationen über das Thema Sicherheit und Unternehmensschutz, Erkenntnisse der Sicherheitsbehörden hinsichtlich Wirtschaftskriminalität und -Spionage schärfen das Sicherheitsbewusstsein der Mitarbeiter und deren Willen, die eingeführten Sicherheitsmaßnahmen zu unterstützen. Ganz gleich ob Safety oder Security - die Mitwirkung der Mitarbeiter ist unabdingbar.