

Pressemitteilung

Defense AG erweitert Portfolio um Human Factor Risk Assessment

„Menschliche Faktoren“ im Risikomanagement

Ismaning, 16. September 2009: Der IT-Security-Dienstleister Defense AG hat sein Lösungsportfolio erweitert und bezieht in seine Risk Assessments neben einer Überprüfung der technischen Schwachstellen zukünftig auch die „menschlichen Faktoren“ mit ein. Die Defense AG ergänzt damit ihre bestehenden Dienstleistungen wie Security Audits und Security-Empowerment-Kampagnen.

Risikomanagement ist für Unternehmen Pflichtprogramm. Nur wenn Unternehmen die mit dem eigenen Business verbundenen Risiken kennen, sind sie in der Lage, diese einzugrenzen und die Ausgaben für Sicherheit gezielt auf die tatsächlichen Gefahren abzustimmen. Besonders schwer einzuschätzen sind dabei erfahrungsgemäß die Risiken, die aus dem Verhalten oder mangelnden Wissen und Können der Mitarbeiter und Führungskräfte resultieren. In ein Risiko-Assessment, das diesen Namen verdient und von Partnern, Kunden, Banken und Gerichten anerkannt wird, müssen daher die „menschlichen Faktoren“ ebenso einbezogen werden wie technische Schwachstellen.

Die Defense AG untersucht die nicht-technischen Einflüsse, die die Sicherheitskultur eines Unternehmens bestimmen, in Zusammenarbeit mit Wissenschaftlern der Universität München.

Die Methodik der Risk-Assessments stützt sich auf Analysen der Kommunikation, Befragungen und Gespräche. Forensische Untersuchungen der Kommunikationsströme und Analysen der Benutzerschnittstellen für Anwendungen können einbezogen werden. Alle Elemente sind standardmäßig anonymisiert, um Konflikte mit Datenschutz-Anforderungen auszuschließen. Das konkrete Vorgehen erläutert Dr. Johannes Wiele, Senior Consultant bei der Defense AG und Spezialist für Security Empowerment Konzepte:

„Unternehmen erhalten von uns eine ausführliche Analyse, die Handlungsempfehlungen auf technischem und menschlichem Gebiet gibt. Bei der Analyse der „menschlichen Sicherheitsfaktoren“ in Unternehmen betrachten wir zunächst das jeweilige Geschäftsmodell und schließen daraus auf die Anforderungen an den Umgang der Mitarbeiter mit Daten und Informationen. Eine Bank hat hier sicher ganz andere Anforderungen als beispielsweise eine Gießerei. Anschließend überprüfen wir, ob die bestehenden Sicherheitsrichtlinien zum Geschäftsmodell passen und auch technisch richtig umgesetzt sind – ob sie zum Beispiel genug Kontrolle oder aber Freiheit bieten, Prozesse nicht behindern und den Kommunikationsanforderungen der Mitarbeiter gerecht werden.

Außerdem analysieren wir die Einstellung der Mitarbeiter zu Informationssicherheit und Datenschutz sowie deren Wissen, Können und Verhalten. Danach klären wir, ob die zur Verfügung stehenden Werkzeuge das richtige Verhalten der Mitarbeiter unterstützen und ob das Management befähigt ist, die richtigen Sicherheitsentscheidungen zu treffen. Nicht zu vernachlässigen sind dann auch noch Fragen zur internen Unternehmenskultur, zu landeskulturellen und regionalen Einflüssen sowie zu aktuellen Krisenfaktoren. Ein weites Feld also, das bisher viel zu sehr von technischen Fragestellungen verdrängt wurde.“

Defense AG – Kundenorientiert durch Innovation

Spezialisiert auf Planung, Entwicklung und Realisierung kundenorientierter Informationssicherheitslösungen bis hin zu Finanzierung und Leasing bietet die Defense AG auf individuelle Kundenbedürfnisse abgestimmte Gesamtkonzepte zur Absicherung von IT-Infrastrukturen. Langjährige Projekterfahrung bei Groß-/Industriekunden sowie die ISO 27001 Zertifizierung machen das Unternehmen zu einem kompetenten, innovativen Partner in der Umsetzung intelligenter Informationssicherheitskonzepte zum Schutz des geistigen Eigentums, Erhaltung der Wettbewerbsfähigkeit, Erfüllung regulatorischer Vorgaben, Betriebsrisikominimierung sowie Betriebskostenoptimierung.

www.defense-ag.de

Redaktionskontakt:

Susanne Pawlik
Defense AG
Reichenbachstrasse 2
85737 Ismaning b. München
Tel: 089. 89 74 64-0
Fax: 089. 89 74 64-64
www.defense-ag.de
susanne.pawlik@defense-ag.de