

Mit der IT-Sicherheit immer alles gut gegangen? Das gute Gefühl auf die Probe stellen

Wie oft hört man über Bedrohungen der IT und stellt fest, dass „bei uns“ nichts passiert ist? Alles gut gegangen! Sicherheitssysteme inklusive Firewall laufen ja!

Alles sicher!? Klar, wir haben ein gutes Gefühl aber es ist und bleibt ein Gefühl. Die Gewissheit fehlt.

Nichts ist in der IT so stetig wie der Wandel. Ein sicherer Status kann urplötzlich durch Bedienfehler, Patches und neue Gefahren ganz anders aussehen. Wer kann schon ständig darauf achten und prüft das sichere Gefühl im Tagesgeschäft?

Es bleibt nur wenig Zeit für Sicherheitsaufgaben etwa gemäß Grundschutzhandbuch, von Budget- und Personalkürzungen ganz abgesehen.

Viele Organisationen haben spezialisierte Dienstleister, die sie fachlich differenziert unterstützen. Ein Schritt in die richtige Richtung!

Vorsorge beugt Fehleinschätzungen vor und hält den Rücken frei

Einen Schritt weiter geht, wer mit seinem Dienstleister Parallelkompetenzen für die Sicherheit aufbaut – eine Co-Competence also. Dies ermöglicht, das Tagesgeschäft im Griff zu haben und Prozesse zu unterstützen. Gleichzeitig hat man einen steten Blick auf den Sicherheitsstatus. Optimal er-

scheint ein Co-Competence-Modell, das sich flexibel an Budget und Anforderungen im Unternehmen anpasst.

Gemeint sind Funktionen, die den gesamten Sicherheitsprozess unterstützen und einer permanenten Sicherheitsüberwachung mit Warnfunktion entsprechen – ähnlich einem Seismographen, der beobachtet, warnt und so zusätzlich zeitnah IT-Risiken eliminieren kann.

Sicherheit nach Maß statt überlademem Aktionismus

Der gesamte Unterstützungsbedarf von Beratung und Analyse über Monitoring, Umsetzung und Betrieb kann mit Co-Competence abgedeckt werden. Wichtig ist ein gesunder Pragmatismus, der IT-Sicherheit ganzheitlich aber nicht wissenschaftlich überspannt betreibt.

Co-Competence integriert sich zeit-, geldsparend und ohne Belastung des IT-Personals. Den Rücken frei für Kernkompetenzen hat die IT, wenn das Sicherheitsgefühl nicht nur co-kompetent hinterfragt, sondern auch transparent gehalten wird.

Indem Relevanzkriterien für eine prämiensbasierte Abrechnung herangezogen werden, kann Co-Competence in Zeiten knapper IT Budgets umgesetzt werden.

Co-Competence funktioniert ähnlich wie

das Gesundheitssystem, wo (noch) regelmäßige kostenfreie Vorsorgeuntersuchungen möglich sind und eine etwaige notwendige Therapie erst nach Diagnose und Aufklärung des Patienten erfolgt. Sowohl Prämienmodelle als auch Festpreise helfen anschließend, eine wirtschaftlich sinnvolle Sicherheitstherapie zu betreiben.

Infobox

Diese Leistungen können co-kompetent und relevanzorientiert integriert werden

- Penetrationstests
- Sicherheitsaudit und Analysen
- Warn- und Vorsorgefunktionen
- Datenschutz
- Managed Services
- Assurance-Programme
- Sicherheitsrichtlinien

Der Autor ist Inhaber des Sicherheitsdienstleisters adMERITia. Mit innovativen Dienstleistungen integriert sich adMERITia mit außerordentlichem Nutzen bei ihren Kunden. Die Berater eliminieren Risiken wirtschaftlich sinnvoll und pragmatisch über den Gesamtprozess. Rund 100 Kunden denken an adMERITia, wenn sie an IT-Sicherheit denken. adMERITia ist auf der CeBIT in Halle 7 (Stand A47) auf dem Partnerstand des DATAKONTEXT-VERLAGES und hält dort Vorträge über Real-Hacking.

Heiko Rudolph

