RISK DOCTOR BRIEFING

Risiken der Computerkriminalität managen

© *May 2014, Ben Rendle*

ben.rendle@rioscaconsulting.co.uk

Computerkriminalität (Cybercrime) ist eine rasch wachsende Bedrohung der Weltwirtschaft. Aber sie ist nicht klar definiert und wird häufig mit Cyberkrieg (Cyberwarfare) oder Cyberterrorismus (Cyberterrorism) verwechselt. Risikoprofis müssen Computerkriminalität sowie ihre Verbindungen zum Risikomanagement verstehen, da wir beim Widerstand gegen diese wesentliche Bedrohung von Wirtschaft und Gesellschaft wertvolle Hilfe leisten können.

Einige Risikoprofis denken, dass Computerkriminalität nur für Techniker relevant ist und dass sie von den IT-Abteilungen angegangen werden sollte. Aber Computerkriminalität stellt ein signifikantes Risiko für Organisationen dar, da sie ihre Fähigkeit beeinflusst, strategische und operative Ziele zu erreichen. Unglücklicherweise wissen viele Unternehmen nicht, wie Computerkriminalität aussieht, wie wahrscheinlich sie von ihr betroffen werden, wie groß ihre Auswirkungen sein können oder wie man sie am besten handhabt.

Computerkriminalität kann Organisation auf viele verschiedene Arten und Weisen treffen, einschließlich

- Online-Diebstahl oder -Betrug
- Identitätsdiebstahl
- Erpressung
- Diebstahl von Kundendaten
- Diebstahl von intellektuellem Eigentum
- Industriespionage

Wie stark eine Organisation durch Computerkriminalität gefährdet ist, hängt vom Grad ihrer Onlineaktivitäten ab. Dies schließt das Ausmaß ihrer Onlinepräsenz, das Maß, indem wertvolle Assets und Informationen online gespeichert werden, die Stärke ihrer Onlinesicherheit und den Grad des Risikobewusstseins in der Organisationskultur ein.

Um das Risiko der Computerkriminalität zu managen, müssen wir erst den Grad unserer Onlineaktivitäten bestimmen und außerdem, welche Assets und Aktivitäten von Computerkriminalität betroffen sein könnten. Danach können wir anfangen, unsere Computerkriminalitätsrisiken zu identifizieren, zu bewerten und zu managen. Die folgenden Schritte helfen dabei:

- **Klares Verstehen und Definieren der organisatorischen Ziele der Onlineaktivitäten.** Erkennen der spezifischen und unterschiedlichen Onlineumgebungen unserer Stakeholder sowie die Bewertung ihrer Einstellung zu Online-Risiken.
- **Kulturelle und technische Faktoren adressieren.** Dies schließt kulturelle Hindernisse, Kommunikationsschwierigkeiten und die Auswirkungen von Voreingenommenheiten bei der Wahrnehmung von Computerkriminalitätsrisiken ein.
- **Erkennen von internen und externen Bedrohungen durch Computerkriminalität.** Interne Bedrohungen können durch Mitarbeiterfehler, versehentlichen Datenverlust oder böswillige Lecks sensibler Firmendaten entstehen. Externe Bedrohungen können durch Hacker, Interessenvertretungen, Wettbewerber oder sogar feindliche ausländische Regierungen sowie durch Viren, Würmer, Trojaner etc. entstehen.
- **Klären Sie Verantwortung, Haftung und Anreize, um Computerkriminalitätsrisiken zu adressieren.** Das gesamte obere Management sollte für das Management der Computerkriminalitätsrisiken in ihrem jeweiligen Verantwortungsbereich haftbar sein und wir sollten die Stakeholder hinterfragen, dies es „als nicht mein Problem“ ansehen.
- **Computerkriminalitätsrisiken innerhalb eines Enterprise Risk Management (ERM) Frameworks managen.** Computerkriminalitätsrisiken können das gesamte Unternehmen in Bereichen wie Ruf, Geschäftskontinuität und Dominoeffekten bei Zulieferern und Subunternehmen betreffen. Daher müssen sie als Teil unserer gesamten Risikoantwort einheitlich angegangen werden.
- **Entwickeln einer globalen Perspektive der Auswirkungen von Computerkriminalitätsrisiken.** Viele Organisationen sind von der Wirtschaft in anderen Ländern abhängig für Handel, Export und Gewinnerzielung und dies setzt sie der ausländischen Computerkriminalität aus, die nicht ignoriert werden kann.

Als Risikoprofis müssen wir Computerkriminalität in unserem Denken und unserer Praxis berücksichtigen. Nur so können wir unseren Organisationen praktische, zielführende Ratschläge geben, um die Bedrohung zu reduzieren und unsere Geschäfte zu schützen.

To provide feedback on this Briefing Note, or for more details on how to develop effective risk management, contact the Risk Doctor (***info@risk-doctor.com***), or visit the Risk Doctor website (***www.risk-doctor.com***).

Aus dem Englischen von Thomas Wuttke (www.thomaswuttke.com)