Die EU-Datenschutzverordnung sollte deshalb so angepasst werden, dass sie die hier genannten Anforderungen anstelle der bisherigen Vorgaben enthält.

Information Security Forum veröffentlicht Threat Horizon 2015

Das Information Security Forum (ISF, www.securityforum.org), eine der weltweit größten Organisationen für Informationssicherheit, Cybersicherheit und Risikomanagement, veröffentlichte am 27.02.2013 seinen Threat Horizon 2015. Das größte Sicherheitsrisiko für Unternehmen geht demnach weiterhin von bereits bekannten Faktoren wie organisierter Cyber-Kriminalität, Social Engineering, mobilen Geräten, Social Media, Cloud Computing, Malware und dem mangelnden Bewusstsein für diese Gefahren aus. Gleichzeitig steigen das Entwicklungsniveau und die Komplexität der von diesen Faktoren ausgehenden Risiken stetig, womit die meisten Unternehmen nicht Schritt halten können. Das ISF fordert Unternehmen deshalb dazu auf, ihr Risikomanagement so zu gestalten, dass sie jederzeit flexibel auf Veränderungen bei bekannten und neuen Bedrohungen reagieren können.

Die jährlichen Threat Horizons des ISF geben Unternehmen einen Überblick über die IT- und Cyberbedrohungen der kommenden Jahre und bieten Handlungsempfehlungen, wie diese sich frühzeitig darauf einstellen können. Die Berichtsserie adressiert insbesondere das Top-Management und die IT-Sicherheitsverantwortlichen in Unternehmen. Eine Kurzzusammenfassung steht unter *www.securityforum.org/downloadresearch/publicdownloadth2015* zum kostenlosen Download bereit.

Die wichtigsten Themen des Threat Horizon 2015 im Überblick:

Stellenwert von Cybersicherheit beeinflusst das Risiko
Das Sicherheitsrisiko von Unternehmen hängt stark davon ab, welchen Stellenwert sie Cyber- und Informationssicherheit einräumen. Unternehmen, bei denen das Thema nicht zum Zuständigkeitsbereich der Geschäftsführung gehört, haben langfristig ein erhöhtes Risiko für Datenverluste und andere Zwischenfälle. Auch durch das Outsourcing der Informationssicherheit erhöht sich langfristig das Sicherheitsrisiko. Unternehmen verlieren dadurch die Kontrolle und können nicht mehr eigenständig auf Änderungen der Bedrohungslandschaft reagieren. Sie sollten sich deshalb frühzeitig um den Aufbau interner technischer und personeller Ressourcen kümmern.

Unternehmensreputation im Visier
Cyberattacken und Hacktivisten haben verstärkt die Reputation von Unternehmen im Visier. Um einem Unternehmen nachhaltig zu schaden, ist es nicht mehr notwendig, es lahmzulegen. Es genügt heute bereits, den Ruf eines Unternehmens zu schädigen. Cyberspace und Internet machen es Cyberkriminellen und Hacktivisten sehr leicht, an kritische Informationen zu gelangen und diese zu verbreiten.

Cyberkriminelle taxieren den Wert von Informationen
Crime as a Service (CaaS) erreicht ein neues Niveau. Cyberkriminelle wägen genau ab, welche Personen im Unternehmen Zugang zu wertvollen Informationen haben und damit potenzielle Einfallstore bieten. Dabei entwickeln sie immer ausgefeiltere Methoden, um die verbesserten Sicherheitsmechanismen von Unternehmen zu überwinden. Sie setzen dabei verstärkt auf eine Kombination von Social Engineering und ausgefeilter technischer Methoden.

Tempo der technischen Entwicklung birgt erhebliche Risiken
Das erhöhte Tempo des technologischen Fortschritts verschärft die Sicherheitslage. Trends wie BYOC (Bring Your Own Cloud) und BYOD (Bring Your Own Device) bergen neben Chancen auch erhebliche Sicherheitsrisiken für Unternehmen. Die Gefahr besteht einerseits darin, dass Technologien eingesetzt werden, ohne vorher ausreichend getestet worden zu sein. Andererseits werden Informationen häufiger dupliziert, an immer mehr Stellen abgelegt oder sind über immer mehr Devices zugänglich. Unternehmen verlieren dadurch leicht den Überblick und bieten Angreifern mehr Angriffsmöglichkeiten.

Unternehmen dürfen sich nicht auf ihre Regierungen verlassen
Zwar nehmen staatliche Aktivitäten im Kampf gegen Cyberkriminalität eine Schlüsselrolle ein, nichtsdestotrotz müssen sich Unternehmen eigenverantwortlich schützen. Sie können und dürfen sich nicht auf den Gesetzgeber verlassen, sondern müssen eigenständig eine auf ihre individuellen Begebenheiten zugeschnittene Cybersicherheitsstrategie entwickeln und umsetzen.

Video-Beiträge zu alltäglichen IT-Sicherheitsrisiken

In Zusammenarbeit mit dem Landeskriminalamt NRW produziert das Institut für Internet-Sicherheit – if(is) professionelle Video-Beiträge, die verschiedene IT-Sicherheitsrisiken veranschaulichen.

Ziel der Zusammenarbeit ist es, das Bewusstsein für IT-Sicherheit zu schärfen – sowohl bei Privatanwendern als auch bei Unternehmen. So zeigen die Video-Clips beispielsweise, wie einfach sensible Daten aus einer Anwaltskanzlei gestohlen oder Besitzer von Smartphones auf Schritt und Tritt ausspioniert werden können.

Das Landeskriminalamt und das Institut für Internet-Sicherheit haben bereits sechs Videos fertiggestellt, die alltägliche Themen aus dem Bereich der IT-Sicherheit addressieren. Besucher des Marktplatzes IT-Sicherheit können nun ab sofort unter *www.it-sicherheit.de/ratgeber/videos/lka_videos/* das erste Video abrufen.

Darüber hinaus bietet die vom Institut für Internet-Sicherheit initiierte Online-Plattform Interessierten weiterführende kostenfreie Informationen rund um IT-Sicherheit.

Aufgrund der großen Nachfrage an Sicherheitstipps im Bereich der IT-Sicherheit, werden derzeit vier weitere Videos produziert. Bis Mai 2013 entstehen damit zehn Sicherheitsvideos in Zusammenarbeit zwischen dem LKA und dem Institut für Internet-Sicherheit.

E-Postbrief bietet Ende-zu-Ende-Verschlüsselung für Berufsgeheimnisträger

Die Deutsche Post kündigte am 01.03.2013 einen erweiterten E-Postbrief vor, mit dem Träger von Berufsgeheimnissen sensible, personenbezogene Daten rechtssicher versenden können. Der „E-