Bedrohte IT-Sicherheit

Angriffe auf die Sicherheit informationstechnischer Systeme sowie Abwehrmaßnahmen standen im Mittelpunkt der IT-Defense 2010 vom 3. bis 5. Februar 2010 in Brühl bei Köln.

Wenn man die Menschen zu täuschen versteht, kommt man in Gebäude oder in Computersysteme auch ohne spezielle Ausrüstung oder Werkzeuge hinein“, referierte Sachbuchautor Johnny Long, der sich mit „No-Tech-Hacking“ beschäftigt. „In weiterer Folge kann man Daten und Identitäten stehlen.“ Auf das Beobachten kommt es an. Wie erhalten Berechtigte Zutritt zu Gebäuden oder Räumen? Wie kann man durch unverdächtiges Auftreten Bewachungspersonal überlisten? Aus Computer-Bildschirmen lässt sich, über den aktuellen Inhalt hinaus, durch die verwendeten Symbole für Programme oder durch Auswerten der Taskleiste, vieles herauslesen. Welche Programme werden eingesetzt? Welcher Browser oder welche Suchmaschinen werden verwendet? Zu welchen sozialen Netzwerken besteht eine Verbindung? Sind die Firewall und der Internet-Anschluss aktiviert? Wenn dann noch eine Visitenkarte im aufgeklappten Deckel des Laptops steckt, ist das eine Fundgrube für den „Shoulder Surfer“, der jemandem über die Schulter auf den Laptop blickt.

Zu bedenken gibt Long, dass in vielen Hotels über die Koaxial-Kabel des Fernsehens auch der Internet-Datenverkehr mitläuft, der leicht abgezweigt und „gesnifft“ werden kann. Adressanhänger auf Koffern und Reisetaschen, aufgeklebte Logos und Sticker auf Autos, Computern und Laptops verraten ebenfalls viel über den Besitzer, wie auch das, was im Auto offen herumliegt oder achtlos weggeworfen wird.

Der „Social Engineer“ findet damit Anhaltspunkte, sich in das Vertrauen des Betreffenden einzuschleichen. Die Abhilfe liegt in einer Bewusstseinsbildung und darin, bei persönlichen Kontakten doch immer ein gesundes Misstrauen walten zu lassen.

Bulletproof Hosting. Die organisierte Kriminalität braucht, wenn sie sich im Internet bewegt, eine vor Zugriffen der Ermittlungsbehörden schützende, „kugelsichere“ (bulletproof) IT-Infrastruktur, die von weltweit agierenden Internet Service Providern (ISP) angeboten

Die IT-Defense wird vom IT-Unternehmen Cirusec veranstaltet.

Stefan Strobel.

Volker Kozok.

wird. Nach der Definition des FBI wird von einem „Bulletproof Hosting“ erst dann gesprochen, wenn die kriminellen Dienste mehr als 90 Prozent des Geschäftsumfangs ausmachen.

Es handelt sich um ein Milliardengeschäft, über das entsprechend abgesichert Botnetze betrieben werden, Malware und Spam verteilt sowie Phishing-Angriffe gefahren werden, Kinderpornografie und gefälschte Medikamente angeboten und, etwa über Internet-Poker, Geldwäsche betrieben wird, erläuterte Bundeswehr-Offizier Volker Kozok. Zielgruppen für Angriffe können staatliche Einrichtungen oder Unternehmen im wirtschaftlichen Konkurrenzkampf sein. Der Kunde dieser Unternehmen ist der Angreifer. Er kann nicht nur mit entsprechender Vertraulichkeit, Verfügbarkeit und Integrität der Daten rechnen, sondern auch mit einem Anonymisierungsservice, gesicherter Kommunikation, versteckten Servern und qualitätsgesicherter Schadsoftware. Außerdem werden Wegwerfhandys zur Verfügung gestellt, die nur einmal verwendet werden. Die Hardware ist am letzten Stand. Bei der Software werden die Erkenntnisse der Hacker-Szene genutzt. Schwierig ist es, in solche Unternehmen, die nach außen hin legal operieren, einzudringen.

Ein Unternehmen im US-Staat Delaware wurde am 13. November 2008 in einer konzertierten Aktion der Sicherheitsbehörden geschlossen. Das Spam-Aufkommen ging dadurch weltweit schlagartig um 30 Prozent zurück, erholte sich aber innerhalb von 24 Stunden wieder, da andere Anbieter in die Bresche sprangen. Die Schließung der Firma erfolgte wegen Wirtschaftsstraftaten. Die Verstöße gegen das Computerstrafrecht reichten dazu nicht aus. Angesichts dieser Stärke des Gegners, die bereits an Cyber-Warfare heranreicht, sei es laut Kozok notwendig, die Zusammenarbeit zwischen Industrie, Universitäten, Ermittlungsbehörden und den militärischen Einrichtungen zu stärken.

Krisenprävention. Dipl.-Kfm. Frank Roselieb, geschäftsführender Direktor von „Krisennavigator – Institut für Krisenforschung“ *(www.krisennavigator.de)* analysierte die Krisenprävention und -kommunikation bei Datenskandalen und IT-Security-Problemen, unter anderem an Hand von aktuellen Beispielen der Mitarbeiterüberwachung in Deutschland.

Es gebe zwar Ad-hoc-Krisen, aber die meisten Krisen entwickeln sich. Die potenzielle Krisenphase schafft den Nährboden. Erste Vorzeichen bahnen sich in der latenten Krisenphase an, etwa durch die Verleihung eines „Big-Brother-Awards“ oder die Veröffentlichung eines Schwarzbuchs. In der akuten Krisenphase werden Videoaufnahmen und Protokolle veröffentlicht; es kommt zu Markteinbrüchen, ersten öffentlichen Entschuldigungen und Einschaltung von Behörden. In der Nach-Krisenphase werden Anzeigenkampagnen und TV-Werbung gestartet, mit dem Ziel, Vertrauen zurückzugewinnen. Den Krisenszenarien entsprechen die Reaktionsmuster „Mea Culpa“ – Change – Restart.

Ein gewisses Frühwarnsystem sind Internet-Blogs und es ist nicht unwich-

Fotos: Kurt Hickisch


Andrea Barisani.


Frank Roselieb.


Johnny Long.


Daniele Bianco.

tig, durch „Online-Scouts“ mitzuverfolgen, was und über wen diskutiert wird. Kernbotschaften sollten so vorbereitet werden, dass sie nur mehr an den aktuellen Fall angepasst zu werden brauchen. Rechtsberater helfen gegenüber dem „Court of Law“, vor dem die Unschuldsvermutung von vornherein gilt.

Sniffing. Andrea Barisani und Daniele Bianco führten auf der IT-Defense vor, wie man mit den Mitteln eines Bastlers Datenverkehr mitverfolgen kann. Bei einem dieser Angriffe zapften sie die Datenleitung eines sechspoligen Keyboard-Kabels an und legten die Leitung über einen Widerstand auf Masse (Wasserleitung). An diesem Widerstand konnten, nach entsprechender Filterung vom übrigen Rauschen, die Datenströme abgegriffen und die Signale ausgewertet werden.

Bei einer anderen Angriffsmethode wurde ein Laserstrahl auf die aufgeklappte Rückwand eines Laptops gerichtet und der reflektierte Strahl empfangen. Durch die mechanische Erschütterung beim Schreiben auf der Tastatur entstanden detektierbare Modulationen dieses Strahls, besonders stark beim Drücken der Leertaste, wodurch das jeweilige Wortende markiert war.

Die Zuordnung der empfangenen Signale zu einzelnen Buchstaben oder Ziffern ist zwar schwieriger, kann aber mit statistischen Methoden gelöst werden. Verhindert könnten solche Angriffe werden, indem schon im Keyboard verschlüsseln wird – damit wären auch zwischengeschaltete Datenträger wie der Keyghost nutzlos.

Eine weitere Schutzmaßnahme ist, Laptops in nicht reflektierendem Design verwenden.

IT-Defense. Die vom Unternehmen *Cirosec* seit 2003 jährlich veranstaltete IT-Defense ist ein Treffpunkt von IT-Experten, die von der Hackerszene über IT-Sicherheitsbeauftragte bis zu Behördenvertretern reichen. Die nächste IT-Defense wird vom 9. bis 11. Februar 2011 im *Lufthansa Training und Conference Center* in Seeheim-Jugenheim stattfinden. *Kurt Hickisch*

www.it-defense.de

Fotos: Kurt Hickisch