Was tun bei Angriffen auf mein Unternehmens-netzwerk?

„Strike-Back“

Rechtliche Rahmenbedingungen beim Eskalationsmanagement. Was verbirgt sich eigentlich hinter diesem Begriff?

Eskalationsmanagement beschreibt die unterschiedlichen Reaktionsmöglichkeiten eines Unternehmens auf Angriffe gegen die IT-Security Struktur. Aufgrund des enormen Schadenspotenzials sowie des eng damit verbundenen Imageverlusts durch die stetig wachsende Zahl an Gefährdungsszenarien in der Datenverarbeitung (Hacker-Angriffe, Denial of Service Attacken, Datenspionage etc.) ist eine ausgefeilte Sicherheitsstruktur wichtiger denn je.

Das Eskalationsmanagement definiert u.a. feste Ablaufstrukturen im Unternehmen. Ein „IT-Security Manual“ legt bspw. fest, wie im Falle eines Angriffs auf das Datennetz zu reagieren ist. Nahezu jedes Unternehmen besitzt eine „permanent“ oder zumindest „dial-in“ Internetanbindung und ist damit ein potenziell gefährdetes Angriffsziel. Für ein Unternehmen im Bereich E-Business ist ein funktionierendes Eskalationsmanagement nahezu unerlässlich.

Im Rahmen des Eskalationsmanagements kann zwischen präventiven (d.h. bereits im Vorfeld wirkende) oder repressiven (d.h. erst im Angriffsfall, unterdrückend wirkende) Maßnahmen sowie passiver oder aktiver Gegenwehr unterschieden werden. Entsprechend unterschiedlich fällt auch die rechtliche Einordnung aus.

«Versucht beispielsweise ein externer Hacker, sich Zugang zum internen Datennetz eines Unternehmens zu verschaffen, kann anhand spezieller Sicherheitssoftware der Angriff erkannt, zurückverfolgt und seine Quelle ermittelt werden»

Aktive Abwehr: „Strike-Back“

Aufgrund der nationalen Datenschutzgesetze (BDSG, TDDSG, TDSV) ist das Unternehmen verpflichtet, Präventivmaßnahmen zu treffen, um den Schutz der Datenbestände vor Angriffen Dritter (unbefugte Kenntnisnahme, Veränderung, Löschung etc.) zu verhindern. Technisch erfolgt dies zumeist durch Vorkehrungen wie Firewalls, Kennwortschutz bestimmter Festplatten und Serverpartizipationen, Tools zur Datensammlung und Analyse oder Kryptographie.

Neben rein passiven Ansätzen bestehen Bestrebungen, Angriffe im Rahmen des sog. „Strike-Back“ aktiv abzuwehren. Versucht beispielsweise ein externer Hacker, sich Zugang zum internen Datennetz eines Unternehmens zu verschaffen, kann anhand spezieller Sicherheitssoftware der Angriff erkannt, zurückverfolgt und seine Quelle ermittelt werden. Die aktive Gegenwehr besteht nun darin, den Angreifer selbst durch geeignete eigene Hacking-Maßnahmen auszuschalten. Unabhängig von der Effektivität und dem Nutzen dieser Vorgehensweise ist die rechtliche Zulässigkeit des „Strike-Back“ jedoch umstritten.

Suche nach einer rechtlichen Grundlage

Bei der Suche nach einer rechtlichen Grundlage sind unterschiedliche Ansatzpunkte möglich. Die „European Convention on Cybercrime“ vom 23.11.2001 sieht in Art. 2 ff. vor, dass die unterzeichnenden Staaten Maßnahmen gegen den unberechtigten Zugriff auf Daten oder Netzwerke einführen. Die Convention kann jedoch nicht als Rechtsgrundlage für einen „Strike-Back“ herangezogen werden, da sie keinen Gesetzesrang auf

nationaler Ebene beansprucht. Sie ist umsetzungsbedürftig und stellt lediglich ein interstaatliches Abkommen dar. Dennoch liegt ihr der Gedanke zugrunde, dass eine rechtliche und tatsächliche Handhabe gegen Angriffe auf Daten und Netze gegeben sein muss.

Das deutsche StGB sieht zwar in § 303 b StGB den Straftatbestand der Computersabotage vor. Dieser kann jedoch ebenfalls nicht als Rechtsgrundlage für einen „Strike-Back“ herangezogen werden. Zivilrechtlich bleibt damit, mangels spezieller Vorschriften, nur ein Rückgriff auf die allgemeinen Regelungen des BGB. Die vorsätzliche Bekämpfung eines Angreifers durch ggf. eigenes zerstörerisches Handeln kann beispielsweise als Fremdgeschäftsführung ohne Auftrag eingeordnet werden. Rechtlich lässt sich argumentieren, dass der Angreifer selbst ein Interesse an seiner eigenen Ausschaltung hat, da dadurch der potenzielle Schaden beim Unternehmen klein gehalten werden kann. Überdies spricht dafür auch die Pflicht zur Minderung bzw. Minimierung des Schadens seitens des angegriffenen Unternehmens.
Ob das Unternehmen nun passiv und präventiv – wie gesetzlich z.T. zwingend vorgeschrieben – oder auch aktiv und repressiv gegen Angriffe vorgeht, liegt in erster Linie im eigenen Ermessen. Zu beachten ist, dass die Zulässigkeit des „Strike-Back“ derzeit höchst umstritten und noch juristisches „Neuland“ ist.

Von RA Robert Niedermeier und Stefan Schröcker

Robert Niedermeier:
Rechtsanwalt bei PricewaterhouseCoopers Veltins Rechtsanwaltsgesellschaft mbH, Vorstand für den Bereich Recht bei EICAR.V – European Institute for Computer Antivirus Research, Initiator von: http://www.cybercourt.de/