Thema: **Wenn die Internetkriminalität Privatsache bleibt**
Quelle: **NZZ**
Datum: **10. März 2008**

Wenn die Internetkriminalität Privatsache bleibt

Der Bund strebt einen Mentalitätswandel bei Firmen an

Die polizeiliche Verfolgung krimineller Angriffe auf Informatiksysteme von Firmen findet noch in einem eher bescheidenen Umfang statt. Ein wichtiger Grund dafür ist die Tendenz der Unternehmen, solche Fälle lieber ohne den Staat zu lösen. Mehr Anzeigen brächten eine genauere Klärung der Kompetenzfrage zwischen Bund und Kantonen.

dsc. Der Bundesrat hat kürzlich die Frage der Zuständigkeit bei Fällen von Internetkriminalität mit dem Verweis auf die neue Strafprozessordnung beantwortet, wonach im Allgemeinen Fälle, die mehrere Kantone oder das Ausland betreffen, zur Bundeskompetenz werden können (NZZ 29. 2. 08). Bei der Fahndung nach illegalen, etwa kinderpornografischen Internet-Inhalten wird auf Bundesebene tatsächlich bereits durch die neun Mitarbeiter der Koordinationsstelle zur Bekämpfung der Internetkriminalität (Kobik) auch ohne Anzeigen systematisch nach illegalen Inhalten gesucht - und somit ansatzweise eine Art überwachende polizeiliche Tätigkeit ausgeführt. Diese Arbeit wird in den nächsten Jahren im Bereich des gewalttätigen Extremismus erweitert. Bei den Angriffen gegen die Computersysteme von Firmen (seien es gewöhnliche Server oder ganze E-Banking-Systeme) ergeben sich aber im Moment vor allem aufgrund des Vorgehens der Unternehmen selbst wenige Ansatzpunkte für eine Ausweitung der polizeilichen Ermittlungsarbeit.

Zurückhaltende Unternehmen

«Wir versuchen Firmen davon zu überzeugen, Fälle von Hackerangriffen bei der Polizei anzuzeigen», sagt Marc Henauer vom Bundesamt für Polizei (Fedpol). Die Unternehmen scheuten sich aber meist davor, Anzeige zu erstatten, nachdem sie «ihren» Fall gelöst hätten. Es herrscht die Meinung vor, dass die Polizei gegen die oft international agierenden Internetkriminellen ohnehin wenig ausrichten könne. Oft wird auch eine Schädigung des Images befürchtet, wenn Nachrichten über Angriffe auf die eigenen Systeme an die Öffentlichkeit gelangen würden.

Bei einem grossen, in Zürich domizilierten Unternehmen der Finanzbranche vernimmt man eine weitverbreitete Aufteilung des Problems: Die intern abgewickelte Beseitigung des Schadens und die Einrichtung weiterer Präventionsmassnahmen werden von der als nebensächlich empfundenen «staatsbürgerlichen Pflicht» zur Anzeige bei der Polizei unterschieden. Wenn nun Heinrich Guggenbühl, Chef der Spezialabteilung für Wirtschaftsdelikte bei der Kantonspolizei Zürich, mitteilen kann, dass reine Informatik-Kriminalität nicht so häufig in den Aufgabenbereich seiner Einheit fällt, ist das wohl weitgehend gerade auf diese Praxis der Privatwirtschaft zurückzuführen. Marc Henauer vom Fedpol würde sich wünschen, dass die Kantone von den Unternehmen mit mehr Anzeigen eingedeckt würden, was dann von selbst auch zum Aufbau neuer Ermittlungsdienste führen würde. Eine genauere Aufteilung der Kompetenzen zwischen den Kantonen, allfälligen kantonsübergreifenden Abteilungen und dem Bund dürfte sich bei einer Zunahme der Anzeigen durch die praktische Arbeit ebenfalls herauskristallisieren.

Genaue polizeiliche Zahlen zu den Angriffen auf Firmensysteme gibt es nicht. Jürg Mosimann von der Berner Polizei geht wie viele von einer «grösseren Dunkelziffer» aus. Die personelle Dotierung seines Korps in diesem Bereich habe sich in den letzten Jahren leicht erhöht, so Mosimann. Am meisten Arbeit verursache aber die Auswertung sichergestellter Computer bei der Bekämpfung illegaler Pornografie und nicht die Wirtschaftskriminalität. Ähnlich klingt es bei anderen Polizeieinheiten. Eine personelle Aufstockung findet da und dort statt. In Basel-Stadt steht derzeit die Einrichtung eines IT-Spezialistenteams zur Diskussion; dabei dürfte aber eine Neuorganisation der bisherigen Tätigkeit und nicht eine grössere Erweiterung der Ermittlungskapazität im Vordergrund stehen.

Sowohl bei den Kantonen wie auch beim Bund reichen die bestehenden Mittel im Bereich der Internet-Angriffe vor allem für die Tätigkeit aufgrund von Anzeigen. Fachleute sehen demgegenüber auch Arbeitsfelder polizeilicher Eigeninitiative, etwa bei der Aushebung von Botnetzen (Netzwerke von «infizierten» Computern, die für gemeinsame kriminelle Aktionen genutzt werden können).

Zusammenspiel von Staat und Wirtschaft

Internet-Angriffe haben sich in den letzten Jahren von einer fast sportlich-lausbubenhaften Betätigung von Computerfreaks zu einem weltweiten lukrativen Kriminalitätszweig entwickelt, der Dienstleistungscharakter aufweist - man kann entsprechend versierte Bösewichte für seine Zwecke anheuern. Bei der Prävention, aber auch bei der Bekäm-

pfung dieses Phänomens ist die Privatwirtschaft als Betroffene selbst offenbar am stärksten gefordert. Der Bund spielt neben der Ermittlungstätigkeit im Rahmen der entsprechenden Abteilungen der Bundespolizei unter anderem mit fünfeinhalb Vollzeitstellen die Rolle als neutrale Informations- und Beratungsstelle im Rahmen von Melani (Melde- und Analysestelle Informationssicherung). Rund 60 Firmen in Bereichen wie Energie, Finanzen, Transport, Gesundheitswesen, Telekommunikation, Industrie und Verwaltung nehmen dabei an einem intensiven Informationsaustausch über vergangene, gegenwärtige und zukünftige Bedrohungen teil. Viele Informationen werden auch der breiteren Öffentlichkeit zur Verfügung gestellt. Der Bund garantiert den Informationsfluss, ohne dass dabei Geschäftsgeheimnisse an Konkurrenten weitergegeben werden.

Bei der Aufklärung von Verbrechen im Informatikbereich nehmen zahlreiche Polizeikorps die Dienste von Privatfirmen in Anspruch. Bei der Prävention ist die Rolle der Privatwirtschaft natürlich noch bedeutender. Die Compass Security Network Computing AG in Rapperswil-Jona war nach eigenen Angaben 1999 das erste Unternehmen in der Schweiz, das Computersysteme von Firmen nach Schwachstellen durchleuchtete, und zwar mit eigentlichen Hackerangriffen. In 98 Prozent der Fälle gelinge ein Eindringen in ein Firmensystem, sagt Geschäftsführer Ivan Bütler. Als Schwachstelle erweist sich dabei nicht der eigentliche Firmen-Server, sondern die einzelnen Computer der Angestellten. Bütler und seine 20 Mitarbeiter haben häufig mit einfach anmutenden Tricks Erfolg. So wird an die Personalabteilung eine Mail mit einer ausführlichen Bewerbung geschickt. Ruft der Personalverantwortliche den angelegten Lebenslauf auf, wird unauffällig Malware in den Computer eingespeist - also Programme, die unbemerkt schädliche Aktionen durchführen. Der Angreifer erhält damit Zugang zum Computer und erfährt etwa wichtige Zugangscodes für weitere Nachforschungen. Unsichere Einzelrechner bei den Kunden und nicht etwa Schwachstellen bei den Banken sind laut Bütler neben nicht erkennbar «falschen» Eingabefenstern für Codes und Geldbeträge auch für viele E-Banking-Betrugsfälle verantwortlich.

Gerade das Beispiel mit dem unvorsichtigen Aufrufen von Mail-Inhalten zeigt die wichtige Rolle des Einzelnen bei der Prävention gegen Angriffe. Auffällig sei ausserdem, wie wenig sich gerade kleinere Unternehmen mit der Sicherheit der Informatiksysteme befassten, wie Marc Henauer feststellt. Fahrlässig werden laut der Meinung von vielen Informatikfachleuten beispielsweise in Bauingenieurbüros elektronische Pläne von allen Rechnern aus zugänglich gemacht und so dem Risiko von Manipulationen ausgesetzt. In vielen Fällen dürften Geschäftsleute von Angriffen auf ihre Systeme nur die Resultate erfahren, etwa einen verlorenen Auftrag, bei dem die Konkurrenz über Internet unbefugt Einblick in die Offerten nehmen konnte.

NZZ Online: http://www.nzz.ch