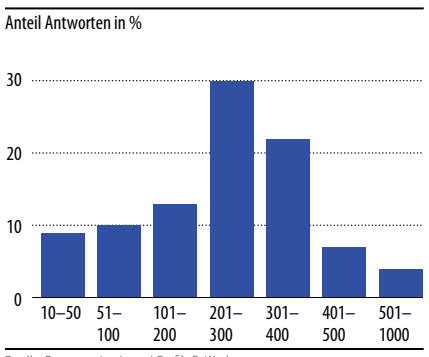
Kosten einer Cyberattacke

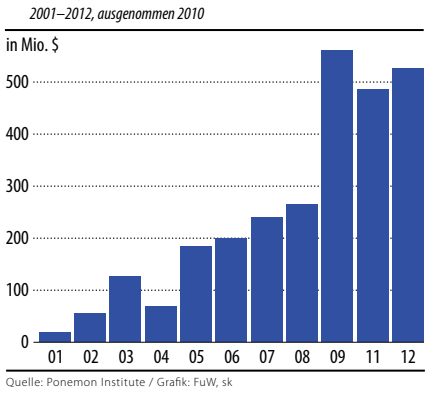
Durchschnittliche Kosten einer erfolgreichen Cyberattacke für ein US-Unternehmen 2012 in 1000 $



Quelle: Ponemon Institute / Grafik: FuW, sk

Schäden durch Cyberkriminalität

Durch Cyberkriminalität verursachte Schäden in den USA
2001–2012, ausgenommen 2010



Quelle: Ponemon Institute / Grafik: FuW, sk

Das Geschäft mit der grossen Angst

INTERNATIONAL Cybersicherheit ist nach dem NSA-Skandal in aller Munde. Für die Branche wird das aber nicht zum Selbstläufer.

THORSTEN RIEDL

Der Feind kommt unbemerkt, am helllichten Tag. Er überwindet die digitale Brandmauer, schaltet sich auf die Rechner – nimmt Einblick in Unterlagen. Er kopiert Informationen, die er braucht. Erst Wochen später weist ein Berater den Industriekonzern auf den Einbruch über das Datennetz hin. Und das ist bei weitem kein Einzelfall.

Laut Statistik der Sparte Unternehmenssicherheit von Hewlett-Packard (HP) bemerken 94% der attackierten Unternehmen einen Angriff von Cyberkriminellen nicht selbst. Schlimmer noch: Im Schnitt vergehen nach einem Einbruch 210 Tage. «Wer ist der Feind?», fragt Marcel Rölli, Sicherheitsspezialist und Verkaufsberater bei HP Schweiz. «Früher waren das Individualisten, heute hat das ganz andere Dimensionen erreicht.» Neben Geheimdiensten suchen sich mafiöse Banden im alltäglichen Cyberwar ihre Opfer.

BILD: KIN CHEUNG/AP/KEYSTONE

Plakat zur Unterstützung von Edward Snowden in Hongkong, der die Überwachungsaktivitäten des US-Geheimdienstes NSA enthüllt hat.

Belebung der Diskussion

Der Skandal um die omnipräsenten Geheimdienste, allen voran aus den USA und Grossbritannien, hat die Diskussion über die Sicherheit von Computernetzen belebt. Nicht einmal vor verschlüsselten Informationen machen NSA, GCHQ & Co. halt. Dazu kommen Hacker, die durch Wirtschaftsspionage ein Auskommen suchen, oder Kriminelle, die Daten zu Geld machen wollen. Der Schaden durch gestohlenes Wissen beläuft sich jährlich schätzungsweise auf 250 Mrd. $. Im digitalen Abwehrkampf helfen Antivirussoftware, digitale Mauern (Firewalls), Einbruchserkennung (Intrusion Detection Systems). Weltweit wird der Markt für Cybersecurity auf mehr als 60 Mrd. $ geschätzt.

Der Bereich wächst laut Marktforschungsinstitut Markets and Markets jährlich mit einer Rate von 11%. Im Jahr 2017 soll er einen Umsatz von 120 Mrd. $ erreichen. 4 von 10 $ für den Cyberschutz kommen aus den USA. Allein die US-Bundesbehörden geben 10 Mrd. $ pro Jahr für digitale Sicherheitsmassnahmen aus, das Gros davon für Beratung. US-Präsident Barack Obama selbst hat das Thema ganz oben auf die Liste gesetzt.

Wenige Unternehmen haben nach dem NSA-Skandal ihre Sicherheitsinvestitionen so publik gemacht wie Petrobras. Der staatliche Energiekonzern Brasiliens hat angekündigt, bis zu 9 Mrd. Fr. in den Datenschutz zu stecken. Das lateinamerikanische Land stand im Fokus der Spionagebemühungen der Geheimdienste. Die brasilianische Präsidentin Dilma Rousseff überlegt, ob sie Internetkonzerne verpflichten soll, Daten ihrer Bürger zwangsweise nur auf Netzrechnern im eigenen Land speichern zu lassen. Den Aufbau eines abhörsicheren Systems für E-Mails der Behörden hat sie angekündigt.

Eine digitale Bonanza

Das alles klingt nach einer digitalen Bonanza für Sicherheitsunternehmen, von denen viele ihren Sitz in den Vereinigten Staaten und Israel haben. Allerdings könnten die Aufregung um die Spionage von Geheimdiensten und das gestiegene Bedürfnis nach Schutz an anderer Stelle wieder Aufträge kosten. In den USA erlaubt es der nach den Terroranschlägen vom 11. September erlassene Patriot Act den Behörden, Einblick in Daten zu nehmen – auch von Nicht-US-Bürgern. Internationale Unternehmen würden sich daher nun zweimal überlegen, wo sie ihre Infos speichern, so die Folgerung der Analysten von Forrester Research. Das könnte die US-Cloud-Industrie bis zu 180 Mrd. $ an Umsatz kosten – und indirekt Sicherheitsanbieter treffen. Sinkt der Erlös der Cloud-Provider, müssen sie sparen, eben auch an Schutzmassnahmen.

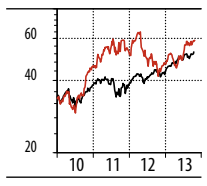
Für Anleger ergibt sich daraus ein diffuses Bild: auf der einen Seite eine Branche mit solidem Wachstum, die durch aktuelle Entwicklungen im Fokus steht – auf der anderen Seite jede Menge Unsicherheit. Hinzu kommt, dass die Branche recht fragmentiert ist. Auf der einen Seite tummeln sich die Grossen. Unternehmen wie Hewlett-Packard und Cisco haben Security zum Wachstumsbereich erklärt. Durch gezielte Übernahmen stärken sich die Konzerne. Auf der anderen Seite stehen kleinere Spezialisten. Teils beflügelt Übernahmefantasie ihre Kurse.

Wie im Fall von Sourcefire. Cisco hat für den Spezialisten für Netzwerksicherheit im Sommer 2,7 Mrd. $ gezahlt. Die Aktionäre erhielten ein Übernahmeangebot mit einem Aufschlag von 29%. Auf einen der grossen Anbieter zu setzen allein wegen seiner Security-Strategie, scheint nicht ratsam. Sie kämpfen oft an anderer Front mit Problemen. Kleinere Titel agieren agiler, profitieren von Übernahmefantasie und verfügen in der Regel über einen treuen Kundenstamm (vgl. Kästen). Das, gekoppelt mit einem soliden Wachstum der Industrie, sollte sich für Anleger mit mittelfristigem Horizont auszahlen.

Mauerbauer

Checkpoint Software

Kurs: 59.67 $
S&P 500 angeglichen



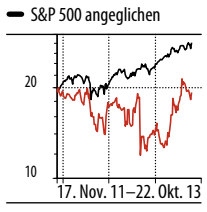
Quelle: Thomson Reuters / FuW

Anfang der Neunzigerjahre wurde **Checkpoint** in Israel gegründet. Damals steckte das Internet noch in den Kinderschuhen. Bekannt wurde das Unternehmen mit Firewalls, also Geräten, die zwischen externem Internet und internem Firmennetz geschaltet werden. Zuletzt ist Checkpoint dazu übergegangen, Software auf Basis eigener Hardware zu bieten. Das hat der Gewinnmarge gut getan. Sie erreichte zuletzt 46%. Jüngst hat das Unternehmen mehrfach die Erwartungen verfehlt. Jetzt sollte es zurück zu alter Stabilität finden. Das Kurs-Gewinn-Verhältnis 2014 liegt bei noch attraktiven 16.

Sicherheitsberater

Booz Allen Hamilton

Kurs: 19.59 $
S&P 500 angeglichen



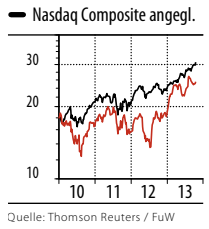
Quelle: Thomson Reuters / FuW

Die Enthüllungen von Edward Snowden, dem berühmtesten Asylanten in Russland, haben **Booz Allen Hamilton** (BAH) geschadet. Das Gros seiner Informationen hat der Whistleblower in seiner Funktion als Angestellter des Beratungshauses gesammelt. BAH arbeitet nicht nur für Geheimdienste. Der grösste Auftraggeber war im abgelaufenen Geschäftsjahr die US-Armee mit einem Anteil von 16% am Umsatz der Berater. Nach den Snowden-Berichten haben die Titel gelitten. Die Sicherheitsbranche bleibt aber beratungsintensiv. Ein Kurs-Gewinn-Verhältnis für 2014/15 von 12 reizt zum Einstieg.

Personenschützer

Symantec

Kurs: 25.41 $
Nasdaq Composite angegl.



Quelle: Thomson Reuters / FuW

Das Softwarehaus **Symantec** gehört zu den Pionieren der Branche, gegründet 1982. Seit Kauf des Back-up-Unternehmens Veritas vor neun Jahren ist Symantec der viertgrösste Softwareanbieter weltweit. Zuletzt harzte es. Im vergangenen Jahr kam ein neuer CEO, Steve Bennett. Er gilt als Fachmann für knifflige Turnaround-Fälle. Symantec ist stark bei Sicherheitslösungen für Privatkunden, ist aber auch im Geschäftskundensegment präsent. Das soll unter Bennett so bleiben. Das Kurs-Gewinn-Verhältnis 2014/15 erreicht derzeit 12. Noch ist nicht die komplette Turnaround-Story an der Börse vorweggenommen. **TR**

«Gefahr böswilliger Eingriffe ins Internet wächst»

Myriam Dunn Cavelty, Cybersecurity-Expertin, äussert sich zur Bedrohung durch Cyberattacken und zu Schutzmassnahmen.

Wachsende Digitalisierung von Daten, zunehmende Smartification von Apparaten und Maschinen sowie steigende Vernetzung: Das sind für Cybersecurity-Expertin Myriam Dunn Cavelty vom Center für Security Studies der ETH Zürich wichtige Gründe, weshalb die Gefahr böswilliger Eingriffe ins Internet grösser wird.

Frau Dunn Cavelty, Cybersecurity ist in aller Leute Munde. Wie gross ist die Bedrohung durch Cyberattacken wirklich?
Die richtige Einschätzung der Bedrohung ist eines der Hauptprobleme in der Cybersecurity-Debatte. Wir wissen, dass die Cyberkriminalität und die Cyberspionage Realität sind, aber es gibt keine brauchbaren Schadenstatistiken, vor allem nicht globaler Natur. Das ist auf Definitionsschwierigkeiten – was ist ein Vorfall? – und auf Messschwierigkeiten zurückzuführen – welchen Schaden soll man wie messen? Hinzu kommt, dass vor allem Spionagevorfälle häufig ganz oder zumindest lange unentdeckt bleiben und/oder von den Betroffenen aus Angst vor Reputationsschäden geheim gehalten werden.

Trotzdem: Wie gross ist die Bedrohung?
Die potenziellen Auswirkungen einer Cyberattacke – die bis zum Stillstand unserer Gesellschaft reichen können – sind sehr gross. Aber potenzielle Auswirkungen sagen nichts über die Wahrscheinlichkeit solcher Vorkommnisse aus. Das nötige Wissen für saubere Risikoanalysen ist zurzeit schlichtweg nicht vorhanden. Unter Experten gehen die Schätzungen

BILD: ZVG

Für Myriam Dunn Cavelty haben staatliche Massnahmen einen unklaren Nutzen.

der Wahrscheinlichkeiten denn auch sehr weit auseinander. Es gibt Experten, die Cyberrisiken für hochgefährlich halten, und solche, die einen ebenso schädlichen Hype feststellen, der zu Panikmache und Fehlinvestitionen führt.

Angriffe aus dem Cyberspace dürften in Zukunft aber wohl häufiger werden?
Gegenwärtig nehmen die Digitalisierung und die Smartification von Gegenständen rasant zu. In Zukunft werden wir von «intelligenten» Dingen und Apparaten umgeben sein, die untereinander und mit dem Internet verbunden sind. Zuverlässigkeit und Verfügbarkeit sind die wichtigsten Kriterien beim Design und beim Unterhalt solcher Technologien. Sicherheit spielte dagegen bisher eine untergeordnete Rolle. Mit der steigenden Zahl der Embedded-Systeme und mit deren wachsender Vernetzung untereinander erhöht sich die Gefahr böswilliger Eingriffe – für Manipulationen oder auch für Spionage gegen Unternehmen und Staaten.

Wie kann man sich schützen?
Gegen die grosse Menge von Cyberattacken kann man sich mit den wohlbekannten Information-Assurance-Massnahmen schützen: Firewalls, Virenschutz, kluges Datenmanagement, Patch Management, Schulung von Mitarbeitenden etc. Nur schon das Bewusstsein, dass der Cyberspace eine Menge Risiken birgt, hilft bei der Erhöhung der Sicherheit. Da jedoch durch all diese Massnahmen keine absolute Sicherheit garantiert werden kann, muss die altbekannte Risikoanalyse ergänzt werden durch Business Continuity Management und Incident Handling oder ganz allgemein Krisenmanagement. Insbesondere gegen APT-Attacken – die Abkürzung steht für Advanced Persistent Threat, also ausgeklügelte und sehr zielgerichtete Schadsoftware – gibt es keinen wirksamen Schutz. Da hilft nur gutes Krisenmanagement.

Wer ist für den Schutz verantwortlich?
Weltweit liegt die Verantwortung bei denjenigen, die die Informationsinfrastruktur besitzen. Auch bei hochkritischen – und meist liberalisierten – Infrastrukturen wird in den meisten Ländern auf Freiwilligkeit gesetzt und über Public Private Partnerships der Austausch über die Cyberbedrohung zwischen Regierungsstellen und Infrastrukturbetreibern gefördert.

Sie geben das Stichwort: Für Regierungen ist Cybersecurity ein Thema geworden.
Je stärker das Thema der Cyberbedrohung als Problem der nationalen Sicherheit angesehen wird, desto lauter werden Stimmen, die mehr Regulierung im Bereich der

«Schon das Bewusstsein, dass der Cyberspace viele Risiken birgt, hilft bei der Erhöhung der Sicherheit.»

Cybersecurity fordern. So wird zum Beispiel in einigen Ländern unter anderem eine Meldepflicht für Cyberattacken diskutiert oder werden klarere Richtlinien für Schutzanforderungen erwogen. Dabei ist bisher aufgrund der Schwierigkeit, die Cyberbedrohung richtig einzuschätzen, weitgehend unklar, ob der Nutzen solcher Massnahmen die Kosten wirklich übersteigen würde.

INTERVIEW: MARTIN GOLLMER

Das vollständige Interview mit Myriam Dunn Cavelty lesen Sie online auf: **fuw.ch/231013-2**