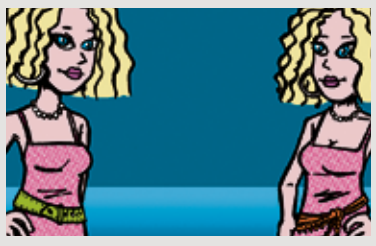
INHALT



Special

Mergers
Wer übernahm wen? Und wie viel wurde bezahlt? Die publizierten Firmenübernahmen mit Schweizer Beteiligung im 1. Halbjahr 2012 im Überblick.

Private Banking Guide

Der «Private Banking Guide 2012» ist ein praxisorientiertes Nachschlagewerk über die Schweizer Private-Banking-Anbieter und zeigt exklusive Anlagevorschläge für typische Kundenprofile auf.

Alle inländischen Einzelabonnenten der «Handelszeitung» erhalten den neuen «Private Banking Guide 2012» kostenlos zugestellt. Zusätzlich zu beziehen ist der Guide zum Preis von 39 Franken (28 Euro) auch über Axel Springer Schweiz AG, Tel. 043 444 59 19, Fax 043 444 50 91, oder per E-Mail: broschueren@axelspringer.ch.

Systemausfälle Pannen und Abstürze nehmen rasant zu. Die Firmen sind überfordert, weil ihre Informatik-Systeme laufend komplexer werden.

Stillstand im Netz

VOLKER RICHERT

Der Auftrag war einfach. Der Banker sollte zum Börsendebüt von Facebook eine Million Aktien kaufen – eine Routineaufgabe. Er drückte auf die Maus, doch die übliche Bestätigung traf nicht ein. Der Mann wiederholte die Order, wieder keine Bestätigung, und dies gleich mehrfach. Was der Banker zu diesem Zeitpunkt nicht wissen konnte – die Informatik-Infrastruktur der US-Börsenbetreiberin Nasdaq kämpfte mit massiven Problemen und war nicht in der Lage, Aufträge zu verarbeiten. Die Server waren dem Ansturm potenzieller Facebook-Aktionäre nicht gewachsen.

Als sich das Problem nach Stunden erledigte, bestätigte das System Nasdaq wie gewohnt automatisch jeden Auftrag – also auch alle ungewollten Mehrfacheingaben des Bankers. Damit hatte sich bei der UBS der Besitz an Facebook-Aktien plötzlich vervielfacht. Da die Kurse einbrachen, resultierte für die UBS ein Verlust von geschätzt 300 Millionen Franken. Die UBS will den Schaden nicht beziffern, teilt jedoch mit, dass sie derzeit Möglichkeiten prüfe, die Differenz zurückerstattet zu erhalten.

Netzwerke als Risikotreiber

Diese kostspielige Panne ist Sinnbild für ein Phänomen, das längst den Alltag prägt. Die noch relativ junge, aber immer komplexer werdende IT-Technik bringt Schweizer Unternehmen an den Anschlag und stellt sie vor immense Probleme. Die Wirtschaft ist mittlerweile total abhängig von der Informatik und dadurch anfällig auf Systemausfälle oder Abstürze, die sich regelmässig ereignen. Gerade zu Beginn dieser Woche fiel das Rechenzentrum im Bundesamt für Informatik und Telekommunikation (BIT) aus und hatte Auswirkungen auf das gesamte Netzwerk.

«Die IT war einst eine Ansammlung von Systemen, welche sich im Firmennetz befanden und von schädlichen äusseren Einflüssen klar abgeschottet waren», erläutert Christoph Baumgartner, Chef des IT-Sicherheitsberaters One Consult. «Noch vor 15 Jahren wussten die Firmen genau, welche Hard- und Software wo und von wem im Einsatz war.» Das Ende dieser Ära leitete zum einen die Nachfrage nach mobilen Arbeitsgeräten ein, zum anderen die massiv höheren Netzwerkbandbreiten, die zunehmende Verlagerung von Geschäftsprozessen ins Internet und die Weiterentwicklung der Virtualisierungstechnologie. Heute legt ein Schädling oder ein Konfigurationsfehler viel schneller als früher die ganze IT-Plantage eines Unternehmens lahm.

So funktionierte im Januar 2012 rund die Hälfte der 600 Bankomaten der CS nicht mehr. Die Kommunikation zwischen der Grossbank und dem Bankomatbetreiber Six Card Solutions war aufgrund eines Serverfehlers knapp drei Stunden lang ausgefallen. Im Februar kämpfte der Telekomanbieter Sunrise mit Softwarefehlern bei der Combox seiner Prepaid-Kunden. Swisscom-Anrufer konnten Botschaften beim Konkurrenten abhören. Im selben Monat konnten die Studierenden der Universität Luzern nicht auf das Online-Portal der Hochschule zugreifen, um ihre Noten abzurufen. Dadurch wussten sie nicht, ob sie überhaupt weiterstudieren konnten. Im März geriet das Universitätsspital Zürich in die Schlagzeilen, weil rund 3000 Patienten Rechnungen für zum Teil Jahre zurückliegende Behandlungen erhielten. Grund für die Panne waren Schnittstellenprobleme zweier Anwendungen.

Wegen der Panne hatte sich bei der UBS der Bestand an Facebook-Aktien vervielfacht.

Neben der Infrastruktur löst gerne eine neue Software Pannen aus. Bei Coop hatte dies im April Folgen fürs Kerngeschäft. Zahlreiche Kassen in der Deutschschweiz liefen nach dem Aufspielen eines Updates stundenlang nicht mehr, sodass die Öffnung vieler Läden verschoben werden musste. Noch schlimmer kann es ein Unternehmen bei der Einführung einer neuen Geschäftssoftware treffen. Im Mai verzögerte sich bei Huber + Suhner die Auslieferung von Waren um einige Wochen, als das Unternehmen flächendeckend auf SAP umstellte und mit Schnittstellenproblemen zu kämpfen hatte. Aufträge, die noch in die alten Systeme eingegeben worden waren, liessen sich im neuen System nicht abwickeln.

Bekannt wurde im Mai ausserdem, dass im Kanton Schaffhausen versehentlich sensible Daten aus dem Migrationsamt und dem Amt für Grundstückschätzungen im Internet landeten. Obwohl das Problem intern relativ schnell erkannt und behoben wurde, blieben die Daten über den Pufferspeicher der Suchmaschine abrufbar. In Bern legten Schwierigkeiten mit Speicherplatten im Rechenzentrum der Bedag die Kantonsverwaltung und die städtische Steuerverwaltung für einen Tag lahm.

Die jüngsten Zahlen des Sicherheitsspezialisten Symantec zeigen, dass nicht nur grosse Unternehmen von solchen Pannen betroffen sind. Im letzten Jahr verlor bereits jedes zweite KMU in der Schweiz Daten. Zudem sind die Firmen bei technischen Störungen häufig vollkommen überfordert. Zwei Drittel haben keine schlüssigen Konzepte, um die Daten im Notfall wiederherzustellen, was im Fachjargon Disaster Recovery heisst. Der Softwarehersteller CA Technologies hat ferner nachgewiesen, dass Netzwerk-, Speicher- und Softwarefehler für rund 70 Prozent der Ausfälle verantwortlich sind. Menschliches Versagen oder ein fehlerhafter Umgang sind zu 41 Prozent für Störungen verantwortlich. Während man den meisten IT-Chefs attestiere, dass sie die Risiken der IT gut kennen, fänden sie offensichtlich nur geringes Gehör in den Teppichetagen, heisst es bei CA Technologies.

International sieht es nicht besser aus, selbst bei den Grossen der Branche. Das Einfügen der sogenannten Schaltsekunde führte in der Nacht zum 1. Juli zu erheblichen Problemen in der Technikwelt. Insbesondere Linux-Systeme und auf MySQL und Java basierende Software waren betroffen, sodass diverse grosse Webseiten nicht erreichbar waren. Die Fluggesellschaft Qantas musste deswegen 50 Flüge verschieben. Mozilla, Betreiber des Firefox-Browsers, Reddit, LinkedIn oder Foursquare waren ebenso betroffen. Ein schweres Unwetter an der Ostküste der USA führte Anfang Monat zu Stromausfällen, die unter anderem ein grösseres Rechenzentrum von Amazon lahmlegten. Cloud-basierte Angebote wie Instagram, Pinterest und der US-Video-Dienst Netflix fielen fast einen ganzen Tag aus. Peinlich war es für den Internetriesen insofern, weil ein falsch aus-

«Cyber-Kriminelle wollen das schnelle Geld»

Attacken Sensible Daten wie Patente im Internet sind laut dem Sicherheitschef der Swisscom eine Einladung an Hacker.

INTERVIEW: VOLKER RICHERT

Marcel Zumbühl
Leiter Sicherheit bei Swisscom

Was ist der grösste Unterschied zwischen Hackerangriffen und technischen Pannen?
Marcel Zumbühl: Im Gegensatz zu Störungen bei technischen Geräten haben Hacker immer ein klares Ziel. Sie wollen möglichst einfach und schnell zu Geld kommen. Ausserdem arbeiten Cyber-Kriminelle fast immer international, auch wenn sie ihre Angriffe auf lokale Ziele richten. Betriebsunterbrüche sind dagegen oft lokale Ereignisse.

Können Hacker Betriebsunterbrüche verursachen?
Zumbühl: Eigentlich nicht. Denn kriminelle Angriffe sind darauf angewiesen, dass die Infrastrukturen ihrer Ziele funktionieren. Es geht ihnen also um Daten, die sich schnell in Geld umsetzen lassen. Ausnahmen bilden allerdings die politisch motivierten Cyber-Angriffe, die man beispielsweise bei dem Computerwurm Stuxnet vermutet, der 2010 Teile der Maschinensteuerung des iranischen Atomprogramms stark beschädigte und zu Ausfällen führte.

Welche Hackerangriffe beeinträchtigen den laufenden Betrieb am stärksten?
Zumbühl: Hier kommt es darauf an, wie sehr ein Geschäftsmodell von einer Online-Anbindung abhängig ist. Webshops, um ein Beispiel zu nennen, müssen ganz besonders gut abgesichert sein. Denn bekanntlich hat die rasante Zunahme an Webportalen in den letzten Jahren auch ihre Attraktivität für kriminelle Angriffe gesteigert.

Sind Veränderungen gegenüber den Vorjahren zu erkennen?
Zumbühl: Grundsätzlich muss man festhalten, dass je virtueller die Gesellschaft wird, desto mehr kommt es zu Angriffen. Je mehr Werte wie Patente, sensible Daten und Prozesse ein Unternehmen ins Internet verlagert, desto stärker verlagern auch professionell handelnde Kriminelle ihre Machenschaften ins Internet.

Wachsen darum auch die Gefahren mit dem Smartphone-Einsatz?
Zumbühl: Ja. Smartphones sind inzwischen zu veritablen Computern geworden, auf denen Unternehmens-Applikationen laufen, Daten gespeichert werden und oft auch Zugangsdaten lagern. Da kann das benutzte Netz noch so sicher sein, die User selbst öffnen durch Bedienungsfehler, Unachtsamkeit, mangelnden Virenschutz und Geräteverlust regelrecht Einfallstore für Kriminelle.

Wo lauern grössere Gefahren, wenn Programme ausfallen oder bei Hackerangriffen?
Zumbühl: Das ist schwierig zu sagen. Wenn geschäftsrelevante Dienste oder ein ganzes Unternehmen stillstehen, weil beispielsweise kein unterbrechungsfreier Betrieb gewährleistet ist, merkt man das in der Regel schnell und kann reagieren. Beim kriminellen Datendiebstahl dagegen wird die Gefahr oft nicht schnell genug erkannt, was unter Umständen viel gravierendere Folgen hat.

Serverraum: Jedes zweite Kleinunternehmen verlor im letzten Jahr Daten.

geführtes Netzwerk-Upgrade bereits im April für Störungen gesorgt hatte. Betroffen von technischen Pannen waren in der Vergangenheit aber schon alle Anbieter von weltweiten Cloud-Services wie Apple, Microsoft oder Google.

Trotz der Häufung von Systemausfällen gibt es noch keine Berechnungen zur Höhe des volkswirtschaftlichen Schadens. Weder beim Wirtschaftsdachverband Economiesuisse noch beim Staatssekretariat für Wirtschaft (Seco) liegen Zahlen vor. Zwar glaubt Roberto Colonnello von Economiesuisse, dass Auswirkungen von IT-Unterbrüchen und -ausfällen «gravierend sein dürften», doch konkrete Studien sind ihm genauso wenig bekannt wie Marie Avet vom Seco.

Parallel zu den Systempannen macht der Diebstahl von Daten übers Internet den Firmen zu schaffen. Unter dem Stichwort Cybercrime sind in der Regel international organisierte Netzkriminelle am Werk, die ihre Angriffe lokal konzentrieren können. Bekannt geworden ist zuletzt der Diebstahl von rund 6,5 Millionen Passwörtern bei der Social-Media-Plattform LinkedIn, die im Internet publiziert wurden und anschliessend erfolgreich genutzt wurden, um sie teilweise – da gleichlautend – für den Zugang zu anderen Plattformen zu verwenden. Kaum anders sah es kürzlich bei der amerikanischen Kontaktbörse eHarmony aus, bei der Hacker 1,5 Millionen Passwörter der Teilnehmer ins Internet stellten.

Gar zum Ruin des Unternehmens führten im letzten Jahr erfolgreiche Angriffe beim holländischen Zertifikate-Anbieter DigiNotar. Hacker hatten es geschafft, in die Systeme von DigiNotar einzudringen und mehr als 500 gefälschte digitale Zertifikate zu erstellen, welche unter anderem zum Ausspionieren von iranischen Facebook- und Google-Nutzern missbraucht wurden. In der Folge wurden sämtliche von DigiNotar ausgegebenen Zertifikate von zahlreichen Softwareherstellern als ungültig taxiert und damit DigiNotar das Geschäftsmodell entzogen.

Firmen ratlos im Umgang mit Cyber-Angriffen

Firmen sind häufig ratlos im Umgang mit Systemausfällen und Cyber-Attacken. Die Krux bei der Risikobewertung liegt laut IT-Sicherheitsberater Baumgartner darin, dass nur auf Erfahrungswerte der Vergangenheit zurückgegriffen werde. Der Kontext, der sich über die Jahre verändere, werde kaum berücksichtigt. So fehle beim Schutz vor Hacker- und Malware-Attacken den Unternehmen oft die Bereitschaft, ihre geschäftskritischen Systeme regelmässig einer technischen Sicherheitsüberprüfung zu unterziehen, um zu erkennen, ob die Systeme vor Angriffen ausreichend geschützt seien. Manche hielten zwar für den Notfall Ersatzgeräte an Lager, vergässen aber, die darauf installierte Software bei Updates der produktiven Systeme auch nachzuführen, was im Ernstfall wertvolle Zeit koste. Eine weitere potenzielle Falle liege bei den Serviceverträgen. Im Notfall hänge, so Baumgartner, die eigentliche Problemlösung vom tatsächlichen Lagerbestand des Anbieters ab. Weil sich die Verträge für den Anbieter rechnen müssen, habe dieser kein Interesse daran, unnötig viele teure Geräte auf Lager zu halten, welche in kurzer Zeit veralten. So kalkuliert der Anbieter spitz und vergleicht die Lagerhaltungskosten mit der Höhe von allfälligen Strafzahlungen bei Nichteinhaltung des Vertrags – ein Umstand, den der Kunde kaum berücksichtige.

Ganz übel werde es, wenn bei überregionalen Schadenereignissen gleichzeitig Dutzende von Kunden auf der Erfüllung der Serviceverträge pochten, der Anbieter sich aber auf höhere Gewalt berufen und sich so aus der Verantwortung stehlen könne, meint Baumgartner. Als weiteren Punkt nennt er sogenannte Notfallpläne, die oft fehlen würden oder veraltet seien. Ganz zu schweigen von regelmässigen Notfallübungen, die nur selten durchgeführt werden, sodass im Ernstfall die nötige Routine fehlt.

«Grundsätzlich stellt fehlendes Risikobewusstsein nach wie vor das grösste Problem dar», sagt Marcus Beyer, Mitverfasser des jährlichen «Security Radar» beim Bassersdorfer Sicherheitsspezialisten Ispin. Erst rund 60 Prozent der Unternehmen weisen ihr Risikobewusstsein als «gut bis sehr gut» aus, wie der demnächst erscheinende «Security Radar» 2012 zeigt. Zwar stellen die Unternehmen rund 50 Prozent ihrer IT-Budgets für den unterbrechungsfreien Dauerbetrieb zur Verfügung, für das Risikomanagement sind es aber noch nicht einmal 20 Prozent. Für Beyer ein unverständliches Verhalten, weil technische Probleme nicht selten auf menschliches Fehlverhalten zurückzuführen sind. Dagegen seien Diebstähle oder Angriffe aus dem Internet eher selten direkt für Betriebsunterbrüche verantwortlich. «Allerdings sind die Folgen auch hier drastisch», warnt Beyer, «weil in der Regel Reputationsschäden und hohe Kosten zur Wiederherstellung der Datenbestände unumgänglich sind.»

INTERNETKRIMINALITÄT

Systematische Angriffe auf Systeme und Online-Betrug

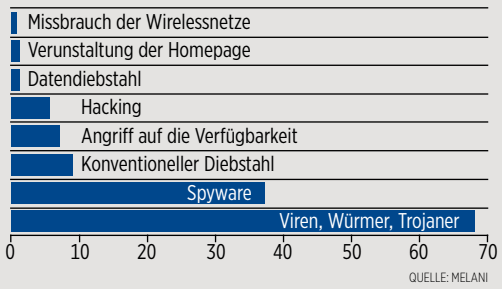
Zwickmühle Generell herrscht das grosse Schweigen und strikte Geheimhaltung. Zahlen existieren nur von den Sicherheitsanbietern. Die Unternehmen stecken in einer Falle. Werden ihre Sicherheitslücken publik, leidet ihre Reputation und sie werden von den Kriminellen erst recht als leichte Beute taxiert.

Betrug Gleichwohl erweitern die Angreifer ständig ihren Aktionsradius. Die Schweizer Melde- und Analysestelle Informationssicherung (Melani) wies zuletzt neben bekannten Angriffsmethoden wie Phishing und Online-Betrug verstärkt erpresserische Schadsoftware, sogenannte Ransomware, aus und Angriffe auf Webshops und Gerätesteuerungen, die mit dem Internet verbunden sind.

Trojaner Gemäss dem Sicherheitsanbieter Symantec haben sich die Gefahrenpotenziale verschoben. In der Schweiz haben Datenspionage (Trojaner) und Boot-Netzaktivitäten, mit denen ganze Rechner gekapert werden können, zugenommen. Als Trend zeichnet sich zudem ab, dass immer mehr KMU ins Visier der Kriminellen geraten – insbesondere dann, wenn sie als Zulieferer tätig sind und als illegale Zugänge zu Grossunternehmen und Konzernen genutzt werden können.

Viele Gefahrenherde

Häufigkeit der Vorfälle (Prozente betroffener Firmen)



QUELLE: MELANI

Computerviren Bereits 43 Prozent der Schweizer User seien Opfer von Cyber-Kriminellen geworden und hätten für die Klärung dieser Straftaten im Durchschnitt fünf Tage aufgewendet. Als die drei häufigsten Angriffsmethoden listet Symantec Computerviren und Schadcode (49 Prozent), Online-Betrug (8 Prozent) und Online-Kreditkartenbetrug (5 Prozent) auf.

Schaden Konkret sind die Ausmasse der Cyber-Kriminalität nur schwer einzuschätzen und man geht von einer hohen Dunkelziffer aus. Symantec weist immerhin am einzelnen User orientierte Zahlen aus. Demnach haben Internetkriminelle in der Schweiz 2011 einen Gesamtschaden von knapp 925 Millionen Franken verursacht (weltweit waren es fast 365 Milliarden Franken). Die Kosten für den Zeitaufwand der Opfer werden dabei mit rund 550 Millionen Franken angegeben und der direkte finanzielle Schaden mit rund 375 Millionen Franken.