

WEB 2.0 wird zur idealen Angriffsplattform Cyber-Crime Community als »Waffenindustrie«

WIEN – Ob es sich um »simple« Datenverlust handelt oder um interne E-Mails, die plötzlich an die Öffentlichkeit gespielt werden, Identitätsdiebstahl in Kombination mit Kreditkartenklau oder durch Denial of Service blockierte Webservices, die Bedrohungspotenziale des Internet sind allumfassend und werden immer komplexer. Die COMPUTERWELT sprach mit Joe Pichlmayr von Ikarus.

Stichwort »Cyber-Kriminalität: Was ist derzeit die größte Gefahr, die im Internet lauert? Viren? Spyware? Drive by Downloads? Trojaner?

Die größten Risiken stecken heute in den Trojanern. E-Mail wird fast nur mehr als Transporteur für URL verwendet – deren Aufruf die eigentlichen »Infektionsprozesse« aktiviert. State of the Art sind mittlerweile mehrstufige Infektionsverfahren, die im Gegensatz zu früheren E-Mail-Outbreaks immer zielgerichteter eingesetzt werden. Erleichtert wird diese »Personalisierung« von Attacken vielfach durch unbekümmerten Umgang mit persönlichen Informationen im Netz – insbesondere auf Web-2.0-Diensten.

Welche neuen Entwicklungen beobachten Sie bei Cyber-Kriminalität? Das Prinzip ist einfach: »make money fast« – dies hat zu einem prägenden Motivwandel geführt. Waren es früher Motive wie Neugier, »me-too«, Langeweile oder Geltungsdrang, so hat sich mittlerweile eine effektive Cyber-Crime Community gebildet, die sich auch erstaunlich »arbeitsteilig« organisiert hat. Neben Daten und Informationen werden ganze Infrastrukturen (Bots, WebServer, Mailserver bis hin zu virtuellen ISP), Software (Trojaner-Codes, Hackingtools) und »Dienstleistungen« (Spamversand, DDOS etc.) angeboten. Firmen – etwa das Russian Business Network (RBN) – bieten »Komplettpakete inklusive Schutz« vor anlaufenden Gegenmaßnahmen allfällig Betroffener an. Die Geschäftsphilosophie ist dabei erstaunlich; so sehen sich die Macher des RBN als Pendant zur Waffenindustrie, da sie selbst keinen Angriff durchführen – sondern eben nur die »Waffen« für Angriffe liefern beziehungsweise bereitstellen.

Was sind die jüngsten Fortschritte bei der Internet Security Technologie? Mit welchen Technologien wappnen Sie sich am besten dagegen?

Revolutionäres hat sich im Bereich der Sicherheitslösungen 2007/08 nichts getan – jedoch lassen sich mehrere Trends ableiten. Neben technologischen Neuerungen, vor allem im Bereich der Umsetzung von Virenschutz- und Security-Maßnahmen, sind aus Kostengründen auch UTM-Lösungen (Unified Threat Management) stark im Kommen. Also »All-in-Ones«-Systeme, die neben Firewall, IDS, Virenschutz und Co. auch entsprechende Policy-Enforcement-Lösungen beinhalten.

Auf der anderen Seite wird aber auch immer mehr in den Bereich »Managed Security Services« investiert. Dabei werden maßgebliche Sicherheitskomponenten an einen Partner (etwa den ISP) »outgesourced«. Auf technologischer Basis rückt das »behavioural blocking« als »Hoffnungsträger« immer mehr in den Vordergrund, auch wenn kritische Stimmen zurecht von altem Wein in neuen Schläuchen sprechen. Es handelt sich hierbei um das Erkennen

von Viren auf Grund deren Verhaltensweisen. Ähnliches wurde schon mit heuristischen Simulationsmethoden versucht. Neu ist jetzt, dass nicht nur der Virencode selbst »bewertet« wird, sondern auch eine »Correlation« dieser Bewertung mit Systemaktivitäten erfolgt.

Mit welchen Bedrohungen werden Unternehmen in Zukunft verstärkt rechnen müssen?

Es ist schon heute eine klare Spezialisierung einzelner Angriffsbilder erkennbar. Attacken mit lokaler Ausprägung werden zur Regel und sind nicht mehr die Ausnahme. Angriffe, die sich gezielt gegen Einzelne richten sind ungleich schwieriger zu erkennen und abzuwehren als der »high-outbreak«, der neben Medieninteresse natürlich auch eine Vielzahl an Security-Experten auf den Plan ruft. Vereinfacht lässt sich sagen, dass sich die Anzahl der Risiken für Unternehmen vervielfachen wird.

Die Optimierung von Abläufen, »Speed to Market« oder »Just in Time« – um nur Schlagworte zu nennen – führt zu einer höheren Anfälligkeit dieser Geschäftsprozesse. Einzelereignisse haben dabei unter Umständen weitreichende Kettenreaktionen zur Folge, die im Kontext der vernetzten Wirtschaft schwer überschaubar sind.

Wie schützt man sich effektiv?

Für Unternehmen gibt es keine Patentlösungen. Immer wesentlicher werden Verhaltensregeln (policies) und Problembewusstsein (awareness). Optional bietet sich auch an, die »ausgetrampelten« Pfade zu verlassen und mit alternativen Systemen weniger »Angriffsfläche« zu bieten. Ansonsten gibt es schon sehr »leistungsfähige« Firewall- und Virenschutzsysteme – neben den schon erwähnte UTM-Lösungen vor allem sehr starke dedizierte Systeme, die allerdings auch einen hohen Spezialisierungsgrad in der »sicheren« Anwendung erfordern.

Absolut auf dem Vormarsch sind Managed Security Services. Sie bieten den großen Vorteil, dass der sehr ressourcenintensive Bereich Security zumindest in operativen Bereichen auf einen Service-Partner übertragen wird. Etwa ein Spamfilter, der schon beim Provider dafür sorgt, dass meine Mailserver die Masse der Spammails gar nicht mehr zu Gesicht bekommt oder mein Surfen im Netz schon ungleich sicherer wird, weil ich über einen zentralen Proxy – etwa bei meinem Mobilfunk-geroutet werde und Trojaner und Viren zum überwiegenden Teil schon zentral abgefangen werden.

Ist mobiles Internet anfälliger für IT-Kriminalität? Wie schützt man sich dagegen?

Nein – ob ich Dienste aus dem Netz über eine fixe Leitung (Kabel oder Festnetz) nutze oder ob ich selbige über mobiles Surfen beziehe, ist für den Angreifer oder meine Anforderung an Sicherheit völlig egal. Es ist nur ein anderer Transport-beziehungsweise Kommunikationsweg, der mich dazu zwingt, ihn in meinen Sicherheitsüberlegungen ebenfalls zu berücksichtigen. Allerdings gibt es auch im Bereich des mobilen Internets tolle Sicherheitslösungen, etwa das A1 InternetSecurity Paket der Mobilkom Austria, das im Vergleich zu anderen Lösungen die Chance bietet, Traffic schon in einem Security-Center der Mobilkom auf Viren und Trojaner überprüfen zu lassen. Und das bietet schon den Vorteil, dass ich damit auf geballtes Abwehr-Know-how zurückgreifen kann und mich nicht mehr selbst

um eine vergleichbare Sicherheitslösung kümmern muss, die ich vermutlich auch nicht mit der selben Effektivität betreiben könnte.

Inwieweit sind Dienst und Plattform des Web 2.0 betroffen?

Mit Web 2.0 wurden das große »Socialising« Zeitalter eingeläutet. Business-Communities wie XING, mit immerhin noch 4,8 Millionen Nutzern, boomen. mySpace, XING und Co. sind die idealen Research-, Manipulations- und Attack-Plattformen für Angreifer. Auf keiner Plattform können Informationen so leicht abgestaubt werden wie hier. So einfach wie im Web 2.0 lassen sich nirgendwo persönliche Daten verknüpfen und komplette Profile von Menschen erstellen. So ermöglicht etwa die Standardfreigabe auf XING unkompliziert die Netzwerke und Aktivitäten von Anwender in und um jene nachzuvollziehen. Die vermeintliche Vertrauensstellung führt dazu, dass das Verhalten von potentiellen Opfern gesteuert werden kann bzw vorhersehbar wird – was weiterführende Attacken ungleich erleichtert und auch die Security Policies von Unternehmen massiv zu unterlaufen vermag. Web-2.0-Plattformen sind die ideale Angriffsplattform für Attacken – auch gegen Unternehmen, in denen die Nutzer von Youtube & Co. ihre Arbeit verrichten. So lassen sich in vielen Fällen Firewalls »tunneln« und Content-Security-Lösungen am Gateway unterlaufen. Die Fülle an Daten, die freiwillig online gestellt werden, wirkt sich auch auf die Qualität von Spam aus. Die Option, E-Mail-Adress-Bücher und ganze PST online zu stellen und mit »Freunden« abzugleichen und zu verlinken, trägt nicht nur unwesentlich dazu bei, dass Spammer reale E-Mail-Adressen einsammeln können, sondern in Verbindung mit anderen Daten auch, dass Spam immer »zielgerichteter« zum Einsatz kommt, und begünstigt zudem »Spear-Phishing« und »targeted Spam«. Einmal völlig davon abgesehen, dass vielen – vor allem jungen Anwendern – kaum bewusst ist, welche Konsequenzen ein informationsreiches »Profil« auf einer jener Plattformen später einmal haben kann – so »schick« es heute auch erscheinen mag. Wie schade, dass ein so genialer Gedanke so zur Falle werden kann. [el]

Das Gespräch führte Edmund Lindau.



ZUR PERSON

Josef Pichlmayr ist geschäftsführender Gesellschafter der Ikarus Software. Er zählt zu den anerkanntesten Virenxperten im deutschsprachigen Raum. 2003 war er Mitinitiator des ersten österreichischen Viren-Frühwarnsystems bei Ikarus im Rahmen von CIRCA (Computer Incident Response Coordination Austria). Heute ist er u.a. für den Betrieb des SOC (Security Operation Center) zur Früherkennung von Phishing-Attacken verantwortlich und hat das A1 InternetSecurity-Paket maßgeblich mit entwickelt.