

"Türen mit Schlössern haben sich auch durchgesetzt"

Interview mit Dr. Klaus Gheri, CTO beim Sicherheitsspezialisten phion AG in Innsbruck.

Lothar Lochmaier

Wie definiert phion den Cyberground oder die Underground Economy, wodurch kennzeichnet sich die heutige Malware-Industrie?

Durch Kommerzialisierung und Industrialisierung der Malware Erzeugung, deren Verbreitung, sowie durch den Aufbau einer mehrstufigen Wertschöpfungskette. Die Szene verarbeitet den aus der Malware erwirtschafteten Nutzen und die Informationen weiter. Die Industrialisierung der Branche hat schon vor einiger Zeit begonnen und wird weiter zunehmen. Da man hier relativ leicht und unbedroht Geld verdienen kann, wird es zu einem weiteren stetigen Anwachsen der Bedrohungen kommen. Die Mehrstufigkeit der Wertschöpfungskette erlaubt es vielen Teilnehmern zudem, ein „reines“ Gewissen zu haben, nach dem Motto: ‚Ich habe mir ja nur Daten geben lassen, aber ich weiß nicht, wo die herkommen‘.

Wie sind Unternehmen mit der Bedrohung konfrontiert, wo liegen in diesem Jahr die größten Herausforderungen in der Corporate Security?

Da moderne Unternehmen in kritischer Weise von der Nutzung von digitalen Kommunikationsmedien und digitaler Informationsverarbeitung abhängen, gibt es eine Vielzahl von möglichen Angriffsvektoren. Am viel versprechendsten für einen Angreifer ist der Vektor über den Webzugang eines Mitarbeiters. Mitarbeiter können über technische Tricks wie Links in E-Mails oder durch bereits kompromittierte Webseiten relativ einfach angegriffen werden.

Viele Mitarbeiter helfen sogar noch aktiv mit, indem sie auf unsichere Seiten oder unsichere Inhalte – Stichwort Messaging oder Filesharing etc. - aktiv zugreifen. Das dual genutzte Notebook oder Multimedia Handy stellt hier ein spezielles Problemkind dar.

Eine weitere Möglichkeit für den Angreifer stellen ungenügend gesicherte Web-Applikationen dar. Bis zu 80 % davon sind aufgrund mangelnden Schutzes durch eine Web Application Firewall in irgendeiner Weise kompromittierbar. Als Alternative bietet sich dem Angreifer die Möglichkeit über gezieltes Social Engineering an, um an spezielle Informationen zu kommen. Dies skaliert jedoch nicht in der Breite und bedingt eine erhöhte Exponierung des Angreifers.

Welche Schutzmaßnahmen können Unternehmen und Endanwender selbst treffen, um ein allzu leichtes Ausspionieren oder Einschleppen von Viren und anderen Schädlingen gezielt zu minimieren?

Viele technische Vorkehrungen können an neuralgischen Übergangspunkten im Netz eingesetzt werden, wobei alle einigermaßen schnell umsetzbar und leistbar sind. Ein Verteidigungskonzept, das mehrstufig ist und vor allem auch den Datentransfer raus aus dem Unternehmen mit einbezieht, kann sowohl das Infektionsrisiko als auch das effektive Schadenspotential stark reduzieren. Wichtig dabei ist die Angemessenheit der Maßnahmen – perfekter Schutz ist meist nicht erreichbar.

Man kommt jedoch bereits mit simplen Dingen einigermaßen weit: Malware-Scans am Proxy bzw.

E-Mail-Gateway, dabei die geschützte HTTPS-Verschlüsselung nicht vergessen werden sollte. Dann gilt es, den Proxy mit Authentifizierung zu betreiben, unerwünschte Protokolle wie Peer-to-Peer/Instant Messaging oder Skype zu eliminieren.

Aber auch getarnte Tunnelprotokolle könne über Perimeter oder interne Firewalls erkannt und geblockt werden. Mein Tipp lautet also: Eine Outbound-Policy an der Firewall implementieren, die nicht beliebige Protokolle nach außen zulässt. Wer einen Schritt weiter möchte, kann über die Ausrollung eines Access Control Agents etwa am Windows-Gerät nachdenken, der laufend das Endgerät hinsichtlich Anti-Virenschutz, oder dem Status rund um die Personal Firewall überwacht und in Abhängigkeit vom Gerätezustand und der Identität des Benutzers im Netzwerk eine rollenbasierte Zugriffskontrolle ermöglicht.

Alle öffentlichen Webapplikationen sollten zudem durch eine Web Application Firewall abgesichert sein. Längerfristig ist zusätzlich ein gutes und regelmäßiges Awareness-Training der Mitarbeiter zu empfehlen, da viele einfache Anwender mit der Thematik schlichtweg überfordert sind.

Welche Schritte sind auf der internationalen Ebene in der Strafverfolgung notwendig. Einige Experten fordern eine Art „Online Interpol“, eine supranationale Behörde, die die ständig sich verändernden Ziele in der Underground Economy besser zu fassen bekäme. Wie steht phion denn zu solchen Forderungen?

Interpol gibt es ja heute schon, das ändert aber nichts an den unterschiedlichen Rechtslagen. Prinzipiell wäre aber eine internationale Zusammenarbeit gegen die organisierte Cyberkriminalität zu befürworten. Dadurch wird sie aber nicht zu existieren aufhören, das hat man bei Drogen und Prostitution nachweislich auch nicht geschafft.

Was also bringen schärfere Gesetze, oder präziser deren konsequente Umsetzung?

Wenn das nur Österreich umsetzt gar nichts. Wir haben jetzt beim Spam schon sehr harte Regeln aber das stört niemanden in Zentralasien. Da man zunächst zwischen gut und böse bei den Nachforschungen nicht unterscheiden kann, ist eine rigorose Ausweitung von Durchsuchungsbefugnissen via Online zur Täterverfolgung nicht ganz unproblematisch. Zudem ist Diebstahl, Betrug, Spionage und anderes jetzt schon strafbar. Das Heil liegt jedoch sicher zunächst darin, sich gegen Bedrohungen adäquat zu schützen – Türen mit Schlössern haben sich ja auch durchgesetzt.

Welche Empfehlungen geben Sie, die Online-Welt sicherer zu machen, so dass E-Business und die freie Kommunikation auf einer soliden Basis stehen können?

Ich plädiere dafür, das Pareto-Prinzip zu beherzigen. Man kann zunächst mit wenig Aufwand viel sicherer werden. Ab einem gewissen Punkt steigt jedoch der zu betreibende Aufwand stark an. Viele Unternehmen haben nach wie vor die richtige Balance im Risikomanagement nicht gefunden und tun zu wenig. Damit bedrohen sie sich selbst oftmals, aber auch indirekt andere, mit denen sie eine Geschäftsverbindung haben. Unsere Empfehlung lautet daher, leicht umsetzbare Maßnahmen sofort anzugehen und sich dann Zug um Zug weiter vorarbeiten. Der ‚alles oder nichts Ansatz‘ geht meist in die Hose.

www.phion.com