DeepSec

Securityconference in Wien.

IT-Sicherheit nimmt an Bedeutung zu. Langsam, aber stetig, stellt auch die Industrie mehr und mehr fest, dass Malware für sie zum Thema wird. Das Internet und die einfache Möglichkeit der Kommunikation und des Datenaustausches sind heute Notwendigkeiten. Die Malware, die man sich damit oft genug einhandelt, hingegen ist das Übel.

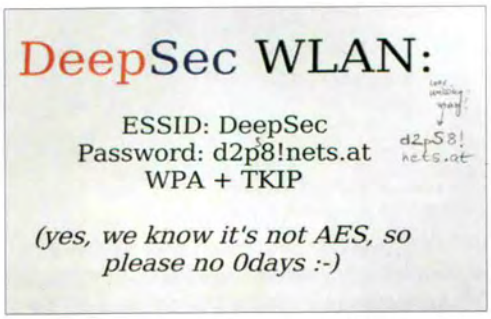
Heinz Liegenfeld

Recht edles Ambiente (oben) und gleich mal die erste kleine Panne humorvoll bewältigt:

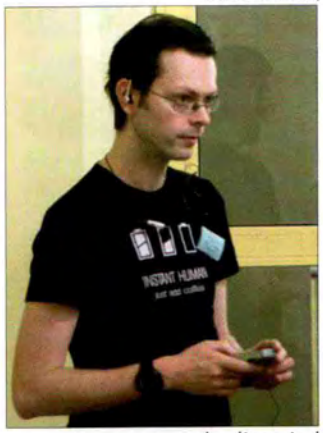
Sicherheitskonferenzen gibt es nicht nur eine. Immer mehr Organisationen und auch Firmen, die die IT-Security zu ihrem Thema machen, veranstalten teilweise riesige Konferenzen, in welchen die IT-Security sich zum Informationsaustausch trifft. Die DeepSec hat ein höheres Ziel.

Weniger Elfenbeinturm, mehr Kommunikation

Statt hier die große Geheimhaltung und eine Aura von Halblegalität zu beschwören, wie dies die alljährliche BlackHat in Las Vegas betreibt, geht die DeepSec sehr direkt in die Öffentlichkeit. Keine Heimlichtuerei, kein Austausch von hochgeheimen Insiderwissen, man versucht Sicherheitsexperten, Akademiker, Wirtschaft aber auch Interessierte an einen Tisch zu bringen und gemeinsam nach Lösungen für die anliegenden und realen Probleme und Bedrohungen zu suchen.



Dies zeigt sich auch in den Vorträgen. Es geht weniger um unbekannte Bedrohungen, deren Potential weder abschätzbar noch real fassbar ist. Die Vorträge drehen sich um reale Bedrohungen, existente Bot-Netze und ihre Auswirkungen, vorhandene Exploits und wie sie ausgenutzt werden, aber auch der Ausblick darauf, welche Bedrohungen sich daraus ergeben.



Organisator Rene Pfeiffer konnte mit seiner Veranstaltung sehr zufrieden sein.

Hands-on statt angewandter Zerebral-Masturbation. Praxis statt grauer Theorie.

Am deutlichsten zeigte sich dies in den Eröffnungsreden. Adam Laurie stellte sehr eindrucksvoll die Probleme der RFID Technologie dar: Wie sie auszuhebeln ist, welche Lücken existieren und warum unser Vertrauen in diverse Techniken deplatziert ist. Das Beispiel, in dem ein Autoschlüssel auf RFID-Basis einfach zu kopieren ist, die Versicherung allerdings jede Leistung ablehnt, weil ja nichts aufgeknackt wurde, eben weil man auf den (*mittlerweile* unsicheren) RFID-Schlüssel vertraute, hat wohl bei einigen zu langen Gesichtern und erheblicher Nachdenklichkeit geführt.

Wie sicher sind unsere als sicher erachteten Technologien? Mehr noch, wie beweist man, dass etwas geknackt wurde, das vom Hersteller *seinerzeit* als „unknackbar" bezeichnet wurde? Ob hier „nur" die Versicherung nicht zahlt oder die Polizei der Meinung ist, ein anderer könnte es nicht gewesen sein, wenn die eigene ID im Spiel ist, ist egal. In jedem Fall ist es wesentlich, solche Sicherheitsprobleme aufzuzeigen und offenzulegen, sonst bleiben womöglich Sie dabei auf der Strecke!

Vertrauen ist gut. Mißtrauen ist besser.

Ins gleiche Horn stieß der andere Eröffnungsredner, Ivan Krstic, der seine Ansprache mit den - gerade vor diesem Publikum - sehr schwerwiegenden Worten: „Die Sicherheitsindustrie hat versagt!" eröffnete. Mißtrauen ist angebracht - gegen jede Technologie. Jede Software und jedes Stück Hardware können ausgehebelt und gegen seinen Benutzer gewendet werden. Keine Technologie ist gegen Manipulation und Mißbrauch gefeit.

Die Kernaussage: Nicht der Computer sollte dem Benutzer mißtrauen, sondern der Benutzer seinem Computer. Und das Kernproblem an heutigen Systemen ist, dass fast alles mit Administratorrechten laufen muss, um überhaupt richtig zu laufen.

Nahezu alle Programme, die der Sicherheit des Rechners dienen sollen, überfordern den User. Es stellt Fragen wie „Das Programm X hat Operation Y versucht? Erlauben oder nicht?" Welcher Otto-Normaluser kann diese Frage in allen Fällen - oder zumindest in den meisten - beantworten?

Seine Ansprache endete mit dem Aufruf an alle, sich dieses Problems bewusst zu werden und, auch wenn es wenig Freude bereitet, sich endlich vor Augen zu führen, dass der User, wenn man ihn mit dem Problem Malware alleine läßt oder ihm untaugliche Mittel in die Hand gibt, dieses Problem nicht lösen kann.

Also ist der Ball bei Microsoft?

Vor allem die von Krstic aufgezeigten Probleme spielen sehr stark in Richtung Microsoft. Das bekannte und oft auch bewitzelte „Allow or Deny" der Vista UAC, wie auch die oftmalige Notwendigkeit, Software mit erheblich höheren Privilegien laufen zu lassen, als dies eigentlich der Fall sein sollte und müsste, spielen beide auf bekannte Probleme mit Microsoft Betriebssystemen an.

Microsoft will die Sicherheit in Zukunft ernster nehmen. Um dies zu unterstreichen, war auch der Leiter des Microsoft Security Response Center, Andrew Cushman (siehe Bild auf der übernächsten Seite), bei der Konferenz in Wien anwesend - mit dem erklärten Ziel, mehr Zusammenarbeit

und mehr Interaktion mit der IT-Securityszene anzubieten und zu erreichen.

Microsoft Security: Ein kleiner Ausblick auf Windows 7

In einem kurzen Interview hat mir Mr. Cushman anschließend einen kleinen Einblick in die security features, mit denen Windows 7 aufwarten wird, geben können. Zu allererst: Microsoft hat verstanden. Das oft kritisierte und auch karikierte Sicherheitssystem von Vista, das den User mehr mit unverständlichen Fragen nervt(e) als für Sicherheit sorgt(e), wird grundlegend umgekrempelt. Microsoft wird dem User in der nächsten Inkarnation des Sicherheitscenters wesentlich bessere und verständlichere Information liefern. Die Fragen werden seltener, das System intelligenter. Gleichzeitig will man an der Benutzerschulung feilen: Microsoft will den User mit dem Wissen ausstatten, das er benötigt, um, wie Mr. Cushman es ausdrückte, eine „informed decision", also eine Entscheidung auf Grund von hinreichender Information, zu treffen. Dies soll sogar für Computerlaien soweit verständlich werden, dass auch diese in der Lage sein werden, ihren Rechner sicher zu halten.

Generell gewann ich den Eindruck, Microsoft setzt zunehmend auf Öffnung und Information. Mehr Information für User, mehr Information für Entwickler, mehr Öffnung zu Leuten, die Sicherheitslücken melden. Die Politik, mögliche Sicherheitslücken bloß nicht publik zu machen, dürfte nun aufgegeben werden. Nicht länger totschweigen, sondern informieren. Ein sehr begrüßenswerter Schritt, da diese Information den Angreifern bisher immer, dem Sicherheitspersonal der betroffenen Firmen oder den betroffenen Privatbenutzern oftmals nicht oder zu spät zur Verfügung stand.

Der Keynote Speaker der DeepSec in Wien: Adam Laurie

Ferner sollen die Tage, in denen Hersteller von Antivirensoftware dazu genötigt waren, selbst wie Trojaner das System zu untergraben und sich in Systemdateien einzuschleusen, vorbei sein. Windows 7 wartet mit einer eigens für diese Probleme konzipierten Schnittstelle für Antivirenentwickler auf, über die Sicherheitssoftware in die Systemprozesse eingreifen können soll. Die Idee dahinter besticht, da damit eine ständige Kontrolle auf Manipulation möglich wird. Es bleibt jedoch abzuwarten, wie diese Schnittstelle gegen Mißbrauch abgesichert wird.

Das zweite Kernproblem von Windows, dass (zu viele) Programme immer noch Administratorrechte verlangen, um zu laufen, kann Microsoft alleine nicht lösen. Die historischen Gründe sind bekannt. Lange Zeit gab es bei den Privatanwenderprodukten von Microsoft, bis Windows98, kein „echtes" User Management, und damit auch kein Sicherheitssystem, das greifen hätte könnte. Schlampiges Programmieren durch Drittanbieter wurde damit natürlich gefördert, da es keine Zugriffsbeschränkungen

gab, in welchen Registry-Tree ein Programm schreiben durfte. Ob in den Tree der „Local Machine", was höhere Privilegien erforderlich machen würde als in den Tree des „Current Users" zu schreiben. Oder ob es gar in den Root-Tree schreiben wollte, was eigentlich die absolute Ausnahme darstellen und eigentlich nur bei der Installation von sehr systemnahen Komponenten stattfinden sollte. All das war irrelevant bei der Entwicklung. Entsprechend scherten sich viele Softwarehersteller wenig um diese „feinen", aber essentiellen, Unterschiede.

Ein interessanter Gesprächspartner: der Leiter des Microsoft Security Response Centers Andrew Cushman

Damit entstand allerdings ein Problem, als die User auf Windows 2000 und XP umstiegen, die beide sehr wohl ein sehr detailliertes Rechtemanagement ermöglichen. Viele Programme liefen nicht mehr, wenn man nicht als Admin den Rechner bediente. Also waren alle User mit Administratorrechten eingeloggt, weil dann „geht es ja". Und da ohnehin wieder alle Administrator waren, hat sich die Schlampigkeit der Softwarehersteller fortgesetzt.

Microsoft kann Softwareherstellern aber nicht vorschreiben, was sie zu tun haben. Hier sind die Hersteller von Software, aber mehr noch die User selbst, gefragt. Microsoft will hier beim User ansetzen und mehr Sicherheitsbewußtsein schaffen, ihm nahelegen, Software zu meiden die unsauber programmiert ist, und mehr Rechte anfordert, als sie zum Funktionieren benötigt. Ob sich dies realisieren läßt, dürfte von den Usern abhängen, und ob sie ihre Sicherheit ernst nehmen.

Die Panzerknacker von TOOOL. Friedlich auf der Couch sehen sie so harmlos aus...

Auch wenn ich über die Sicherheitsfeatures von Vista nicht viel Gutes sag-en könnte, hat mich dieses Gespräch ehrlich optimistisch gestimmt. Sicherheit ist für Microsoft zu einem wesentlichen Thema geworden und ich hoffe, bald ein Testmuster von Windows 7 in den Fingern zu haben, um zu sehen, wie diese Versprechen umgesetzt wurden.

Vor allem frage ich mich, wie die Quadratur des Kreises gelöst werden soll, dem User hinreichend Information zu geben, um die Sicherheit seines Systems in die Hand zu nehmen.

Nicht nur digitale Schlösser werden geknackt

Aber es gibt ja nicht nur Sicherheitsprobleme in der digitalen Welt. Im Rahmen der DeepSec wurden auch sehr reale, handfeste Sicherheitsprobleme behandelt. Deviant Ollam von TOOOL (Bild links unten) stellte Sicherheitsprobleme vor, die man auf einer IT-Konferenz eher weniger erwartet: Das Knacken von Schlössern.

Nein, keine Code- oder Zahlenschlösser, oder anderen High-Tech Kram. Handelsübliche Schlösser wie man sie an Haustüren oder Vorhängeschlössern findet. Wahrscheinlich als Auflockerung gedacht, waren einige der Demonstrationen durchaus „Augenöffner", wie einfach diverse als sicher erachtete Schlösser zu knacken sind und (wie oben bereits erwähnt) wie ungern Versicherungen zahlen, wenn scheinbar nichts wirklich aufgebrochen wurde.

Wichtig ist, was hinten rauskommt

Wie überall ist auch der Erfolg von Sicherheitskonferenzen daran zu messen, welcher Effekt damit tatsächlich erzielt wird. Die DeepSec geht hier, meiner Meinung nach, den richtigen Weg. Es reicht nicht, wenn IT-Security Experten sich zusammensetzen und Probleme diskutieren, ohne dass diese Probleme der Öffentlichkeit, den Firmen wie auch den Privatnutzern von Computern, überhaupt bewußt sind. Es ist leider immer noch selten, dass sich die IT-Securitybranche nach außen öffnet und aktiv Administratoren und Sicherheitsbeauftragte von Firmen anspricht, auch weil oft die Berührungspunkte fehlen. Die DeepSec bietet dies an.

Mir bleibt zu hoffen, dass die DeepSec-Conference uns auch weiterhin erhalten bleibt und es ihr gelingt, mehr Interessierte anzusprechen. Das Niveau der Konferenz war durchgehend sehr hoch, die Vortragenden sehr gut ausgesucht und die behandelten Themen frei von den üblichen eher esotherischen, theoretischen Problemen und konzentriert auf Bedrohungsszenarien, die real aktuell existieren. Es gibt zu viele Sicherheitsprobleme und zu wenig Sicherheitsbewußtsein, vor allem bei vielen davon betroffenen Firmen.

Und betroffen sind alle, die auch nur ansatzweise das Internet nutzen.

Links zum Artikel:

* DeepSec Conference: https://deepsec.net/
* Adam Laurie, RFID und seine Sicherheitsprobleme: http://rfidiot.org
* TOOOL, Lockpicking und andere „Hardhacks": http://www.deviating.net/
* Microsoft Windows 7: http://www.windowsvienna.com/