

Special Innovation

Markus Klemen: „Ein Großteil der Angriffe wird in der Regel von Privatcomputern oder Kleinunternehmen aus gestartet. Oft wissen die Nutzer monatelang nicht, dass ihre Systeme von Trojanern übernommen und für illegale Aktivitäten missbraucht werden“, erklärt der Geschäftsführer von Secure Business Austria.

Stiller Angriff, fatale Wirkung

Sonja Gerstl

economy: Mit ihrem OCG-Sicherheitszertifikat sprechen sie Endnutzer an, die damit ihre eigene EDV-Umgebung sicherer machen sollen. Sollte das Thema Sicherheit nicht besser Profis überlassen bleiben?

Markus Klemen: In unserer heutigen vernetzten Welt ist das leider nicht mehr ausreichend. Ein Großteil der Angriffe – insbesondere sogenannte Denial-of-Service-Attacken, bei denen Zehntausende Rechner ein Zielsystem angreifen, um es zu überlasten – wird in der Regel von Privatcomputern oder Kleinunternehmen aus gestartet. Oft wissen die Nutzer monatelang nicht, dass ihre Systeme von Trojanern übernommen und

für illegale Aktivitäten missbraucht werden. Genau diese Computersysteme müssen besser geschützt werden.

Kann hier ein Zertifikat tatsächlich helfen?

Ein Zertifikat und die damit einhergehende Ausbildung ist natürlich kein Allheilmittel. Aber es kann einerseits zur Bewusstseinsbildung beitragen und andererseits eine gewisse „Grundsicherheit“ bei den Nutzern ermöglichen. Und genau das ist es, was wir damit erreichen wollen.

Hilft diese Ausbildung auch beim adäquaten Umgang mit dem derzeit heftig diskutierten „Bundestrojaner“, also staatlicher Schad-Software?

Das ist eine gute Frage. Tatsächlich ist ja das Platzen eines Trojaners auf dem Zielsystem die eigentliche Herausforderung, sowohl für „normale“ Trojaner als auch für mögliche „Bundestrojaner“. Eine erhöhte Aufmerksamkeit und Vorsicht der Nutzer hat damit zwangsläufig auch darauf eine Auswirkung. Aber da gibt es viele andere Problemereiche, die hier diskutiert werden müssen und die wesentlich relevanter sind. So etwa ist völlig unklar, was passiert, wenn Anti-Virenprogramme einen „Bundestrojaner“ identifizieren und löschen. Ungeklärt ist auch, wie ein sol-



Keine Chance den Hackern: Sicherheitslücken im System bieten ein schier unendliches Betätigungsfeld für böswillige Computerattacken. Foto: Bilderbox.com

cher „Bundestrojaner“ installiert werden soll. Ein E-Mail vom Innenministerium mit der Bitte, sich das angehängte Programm zu installieren, wird wohl nicht zielführend sein. Den Trojaner durch eine Sicherheitslücke im Zielsystem zu installieren, ist jedoch weitaus schwieriger, als man denkt. Vor allem, wenn die Rechner auf dem aktuellen Stand gehalten werden und mit Antivirenprogram-

men und Personal Firewalls ausgestattet sind. Ich denke, hier ist die Politik in ihren Vorstellungen noch in Einklang mit den technischen Möglichkeiten und Problemen zu bringen.

Beschäftigt sich Ihr Zentrum mit Trojanern?

Ja, die Erkennung von böswilligem Programmcode ist ein wichtiger Forschungsbereich, an dem wir intensiv arbeiten. Da-

bei stehen wir vor zwei Herausforderungen: Einerseits müssen wir selbst neue Angriffsmethoden entwickeln oder zumindest bekannte Methoden nachbilden. Andererseits müssen wir Erkennungsroutinen schreiben, die diese Angriffe abwehren können. Wir haben dafür ein separates Fit-IT-Projekt, das exklusiv entsprechende neuartige Technologien erforscht.

www.research.securityresearch.at

Zur Person



Markus Klemen ist Geschäftsführer von Secure Business Austria. Foto: SBA

Sicher durchs Internet navigieren

Ein eigenes Zertifikat soll Nutzern künftig den sicheren Umgang mit Informationstechnologien näherbringen.

Dass das Thema Informationssicherheit für praktisch jeden, der mit Computern arbeitet, immer wichtiger wird, ist offensichtlich. Schließlich sind durch die vermehrte Nutzung internetfähiger Geräte sowohl Privatanutzer als auch kleine und mittelständische Firmen verstärkt herausgefordert, sich ein grundlegendes Wissen bezüglich Gefahrenpotenzial und Schutzmöglichkeiten beim Umgang mit Informationstechnologie anzueignen.

Die Österreichische Computergesellschaft (OCG) hat daher gemeinsam mit Secure Business Austria (SBA), dem österreichischen Kompetenzzentrum für Informationssicherheit, in rund einjähriger Arbeit ein Sicherheitszertifikat samt Lernmaterial entwickelt, das es interessierten Endnutzern ermöglicht, sich essenzielles Know-how an-

zueignen und dieses in Form eines Tests auch zu dokumentieren. Das Zertifikat orientiert sich am äußerst erfolgreichen Europäischen Computer-Führerschein (ECDL), der ebenfalls unter Mitwirkung der OCG entwickelt wurde, und richtet sich im Wesentlichen an die gleiche Zielgruppe.

Training mit Breitenwirkung

„Wir hoffen, mit unserem Projekt einen wichtigen Beitrag zu leisten, um langfristig das Sicherheitsniveau der IT-Landschaft in Österreich zu heben“, erklärt Markus Klemen, Geschäftsführer von Secure Business Austria: „Wir sehen damit die einmalige Chance, durch ein Schulungsprogramm mit abschließendem Zertifikat eine spürbare Breitenwirkung zu erzielen.“ Derzeit werden Zertifikat und Handbuch in Workshops

der OCG den Ausbildnern nahegebracht – im nächsten Jahr sollen österreichweit entsprechende Trainings starten.

„Die Nachfrage von unseren Trainingspartnerunternehmen ist sehr groß und bestätigt uns darin, dass ein solches Programm bislang noch auf dem Markt gefehlt hat“, freut sich

Gabriele Flicker, Programmleiterin der OCG: „Auch das Feedback in den Workshops bisher war sehr positiv.“ Die Kandidaten müssen ein bestimmtes Anforderungsprofil erfüllen. „Das benötigte Grundwissen sehen wir aufbauend auf dem Niveau der ECDL-Core-Ausbildungen. Das heißt, dass die Nut-

zer die wichtigsten Elemente der Betriebssysteme und Programme kennen müssen, um die Prüfung erfolgreich ablegen zu können“, erklärt Flicker.

Ab 2008 soll das Schulungsprogramm samt Zertifikat ausgerollt werden, bis dahin werden noch inhaltliche Feinabstimmungen und Änderungen basierend auf den Ergebnissen der Workshops vorgenommen. „Das Thema Informationssicherheit ist komplex, die besondere Herausforderung liegt darin, teilweise sehr schwierige Inhalte so zu verpacken, dass sie für Endnutzer auch tatsächlich verständlich und umsetzbar sind“, stellt Klemen fest. Zudem soll mit diesem Programm auch die Bewusstseinsbildung bei Unternehmen, Mitarbeitern und Privatpersonen verstärkt werden. sog

www.ocg.at/zertifikate



Die Verantwortung für IT-Security liegt bei jedem einzelnen Mitarbeiter. Foto: Bilderbox.com