Kurzinterview mit Stefan Strobel, Veranstalter der „IT-Defense“

Independence Day für IT-Sicherheit

Vom 12. – 14. Februar 2014 fand in Köln die 12. „IT-Defense“ statt, ein IT-Sicherheitskongress, der den Anspruch erhebt, weitestgehend neutral und herstellerunabhängig zu sein. Im Fokus stehen nicht die Unternehmen mit ihren Produkten, sondern Referenten, die wirklich etwas zu sagen haben sollen. So möchte sich die Veranstaltung von den üblichen, werblich getriebenen Konferenzen abheben. IT-SICHERHEIT sprach mit Stefan Strobel – Geschäftsführer und Gründer der cirosec GmbH – über die „IT-Defense“, die aktuelle Bedrohungslage und die Sicherheit von mobilen Geräten.

IT-S: Wie ist die „IT-Defense“ entstanden? Warum brauchen wir noch eine weitere Veranstaltung zum Thema IT-Sicherheit?

Strobel: Die „IT-Defense“ gibt es nun schon seit zwölf Jahren. Wir haben cirosec 2002 mit neun Leuten gegründet und hatten uns fest vorgenommen, von Anfang an ein paar Dinge besser zu machen. Wir haben uns damals auch über ein Event Gedanken gemacht und festgestellt, dass es in Deutschland tatsächlich keine kommerzielle Sicherheitskonferenz gibt, die internationale Koryphäen einlädt. Es gab zum einen das Jahrestreffen des CCC und zum anderen Sicherheitskonferenzen von den typischen kommerziellen Veranstaltern, die Sponsoren gesucht haben. Das Ergebnis war dann eine Konferenz, auf der das Unternehmen xy einen Vortrag gehalten und ein bisschen Werbung gemacht hat. Wirklicher Benefit für die Leute aus der Szene fehlte.

Auf der anderen Seite gab es damals schon im Ausland sehr viele Hacker-Konferenzen – bekannte sind beispielsweise die „DEF-CON“ und die „Black Hat Briefings“ aus Las Vegas – da haben sich wirklich Profis getroffen. Dort haben Leute aus der Hacker-Szene neueste Erkenntnisse präsentiert, neue Angriffstechniken, neue Schwachstellen. So etwas hat man in Deutschland nur auf dem CCC-Kongress erlebt.

Wir haben diese Lücke gesehen und wollten eine Veranstaltung schaffen, die werbefrei ist, aber dennoch kommerziell-professionell. Sprich, wir wollten ein vernünftiges Hotel als Austragungsort haben, eine sehr gute Verpflegung der Teilnehmer gewährleisten und jeden Tag Abend-Veranstaltungen anbieten, damit sich die Teilnehmer auch austauschen können.

IT-S: Was sind die Themenschwerpunkte der „IT-Defense“?

Strobel: Wir haben immer versucht, eine schöne Mischung zu erreichen, so dass für jeden etwas dabei ist. Das heißt, wir haben einerseits immer ein paar Leute aus der Hackerszene dabei, die über neue Bedrohungen berichten, von denen man noch nichts gehört hat. Auf der anderen Seite haben wir bekannte Buchautoren als Referenten wie beispielsweise den Krypto-Guru Bruce Schneier. Und drittens haben wir immer versucht, Leute mit ins Boot zu holen, die gar keine Technik- oder Security-Spezialisten sind, und mal einen ganz anderen Aspekt aufzeigen können. Bei der Auswahl der Referenten achten wir darauf, dass es auf gar keinen Fall werblich wird. Das heißt, wir laden Referenten ein, die nicht die Interessen einer Firma vertreten, sondern einfach fachlich etwas zu sagen haben.

IT-S: Kommen wir zur aktuellen Bedrohungslage: Verschwindet der Trend, Malware in großer Menge für die breite Masse zu programmieren, und werden dafür weniger, aber hoch gefährliche APTs entwickelt?

Strobel: Diese Aussage würde ich mit Vorsicht genießen. Man muss bedenken, woher solche Aussagen kommen und woher die Presse typischerweise ihre Informationen bezieht. Und die bekommt sie hauptsächlich durch Pressemitteilungen, verfasst von Firmen, die hier ihre ganz eigenen Interessen pushen. Es gibt natürlich ein Wachstum von Malware, die von Profis für gezielte, schwer zu entdeckende Angriffe entwickelt worden ist. Es ist meines Erachtens aber nicht so, dass es deswegen weniger Streu-Malware gibt. Man nimmt APTs einfach stärker wahr, Beispiele dafür waren etwa Stuxnet oder Flame. Daraus ist ein Markt entstanden, in dem Hersteller ihre neuen Produkte verkaufen wollen, die für sich den Anspruch haben, diese fortgeschrittene Malware an ihrem Verhalten zu erkennen. Daher streuen sie Informationen zu dem vermeintlich neuen Trend an die Öffentlichkeit. Jedes Jahr hat so seine Buzzwords, die getrieben werden, um einfach den Konsum anzutreiben.

IT-S: Wo sehen Sie persönlich das größte Gefährdungspotenzial für die nahe Zukunft?

Strobel: APTs sind natürlich dennoch eine große Bedrohung. Das größte Problem ist nach wie vor das Risikomanagement. Jedes Unternehmen muss sich fragen: Was ist für mich eine relevante Bedrohung, vor der ich mich auch schützen kann und möchte? Vielleicht sind das die mobilen Endgeräte, für deren Umgang wir noch keine Richtlinie haben. Oder ist es eine große Bedrohung für mich, dass ich noch immer keine interne Netzwerkzugangskontrolle aufgebaut habe? Die Bedrohungslage ist immer noch sehr individuell, weil viele Firmen gegen bereits vor Jahren bekanntgewordene Bedrohungen noch immer nichts unternommen haben. Des Weiteren sehen wir nach wie vor ein massives Bedrohungspotenzial im Bereich von Web-Shops/Web-Applikationen. Die meisten Unternehmen wissen zwar inzwischen, dass es hier Angriffstechniken wie SQL-Injection oder Cross-Site-Scripting gibt, haben es aber dennoch nicht im Griff, sich davor zu schützen.

IT-S: Wie sieht es mit der Sicherheit von Apps aus? Wann wird Ihrer Meinung nach das Bewusstsein dafür ankommen, Mobilgeräte genauso zu schützen wie einen „normalen“ PC? Viele Leute haben noch nicht mal einen Virenscanner auf ihrem Gerät …

Strobel: Ich glaube, die Sicherheit der mobilen Geräte ist ein schwieriges Feld, auf dem es noch sehr viele Missverständnisse gibt. Virenscanner sind ein sehr schönes Beispiel. Da kommt es nämlich ganz drauf an: Auf einem Android-Smartphone habe ich ein großes Problem mit Malware, ich sollte also unbedingt einen Virenscanner haben. Auf einem Apple-iOS-Gerät hingegen gibt es so gut wie keine Viren. Denn wenn das Gerät nicht gerade gejailbreakt wurde, kann ich Apps ja nur vom Apple-App-Store runterladen, und die Kontrollen im App-Store sind, zumindest relativ gesehen zu dem, was man bei Android von Google kriegen kann, sehr viel besser. Ein Virenscanner wäre hier reine Geldverschwendung. Um zu Apple auch ein paar kritische Dinge zu sagen: Es gibt natürlich noch Leute, die ein iPhone 4 oder gar 3 haben. Viele Besitzer wissen nicht, dass Angreifer diese Geräte mit dem richtigen Equipment in nur zwei oder drei Minuten komplett auslesen können. Sie sind so unsicher, weil sie einen bekannten Fehler im Boot-ROM haben. Dazu kommt der Aspekt Usability, der vielen Leuten immer noch sehr viel wichtiger ist als Security. Viele haben noch nicht mal einen PIN-Code gesetzt, so dass das Gerät von jedem, der es findet, auch direkt verwendet und ausgelesen werden kann.

IT-S: Gibt es etwas, dass Sie jedem IT-Verantwortlichen, der mit sensiblen Daten arbeitet, mit auf den Weg geben möchten?

Strobel: Gehen Sie strukturiert vor. Denken Sie daran, nicht nur einfach auf die Sicherheit zu vertrauen, die vielleicht gar nicht da ist, sondern führen Sie auch mal eine Risikobetrachtung durch, wenn es um sensible Daten geht. Nehmen Sie dafür interne oder externe Spezialisten und überlegen Sie, wie kritisch die Daten wirklich sind und welche Angriffsszenarien dafür denkbar wären. Und fragen Sie sich vor allem, was Ihr Unternehmen eigentlich dagegen unternimmt. Dabei kommen vielleicht interessante Dinge raus.

IT-S: Vielen Dank für das Gespräch!

Das Gespräch mit Stefan Strobel führte Faatin Hegazi, Redaktion IT-SICHERHEIT