Bedrohung aus dem Netz

Bedrohung aus dem Netz

Am 19. Januar 2015 referierte Pascal Lamia, der Leiter der Melde- und Analysestelle Informationssicherheit, am Militär-Campus Luzern über Sicherheit im World Wide Web.

AUS DEM MILITÄR-CAMPUS AM AAL LUZERN RAPPORTIERT UNSER KORRESPONDENT WM PETER GUNZ

Das Sicherheitspolitische Forum Zentralschweiz und Militär-Campus Luzern starteten die Aktivitäten 2015 mit Lamias Referat. Rund 200 Personen lauschten gespannt Lamias Ausführungen.

Alles hat zwei Seiten

Auch wenn das Internet nicht mehr wegzudenken ist, lohnt sich eine genauere Betrachtung von Risiko und Gewinn.

- Das Internet ermöglicht eine globale Kommunikation ohne grossen finanziellen oder personellen Aufwand.
- Das Internet erlaubt neue Kontaktstellen zu Kunden, Lieferanten, Aussenstellen und externen Mitarbeitern.
- Die Informationstechnologie schafft einen schnellen Zugang zu immer mehr, auch businesskritischer, Information.
- Als Träger des *E-Commerce* ist die Informationstechnologie eine strategische Voraussetzung für die Wirtschaft in der Informationsgesellschaft.
- Die Bedeutung der Informationstechnologie wird immer grösser für Geschäftsprozesse und Finanztransaktionen.

Betrug, Spionage, Erpressung

Anderseits steht die Zunahme der Möglichkeiten für Betrug, Spionage, Erpressung. Neue Akteure treten auf. Auch eine Anpassung der Motive und Methoden bestehender Akteure ist erkennbar, für kommerziellen Gewinn oder Know-how-Transfer.

Botnet oder Botnetze

Praktisch allen kriminellen Aktivitäten im Bereich des Internets liegen Botnetze zu Grunde. In Botnetzen sind befallene Rechner zusammengefasst, die von Betreibern zum Versand von Spam-Mails oder Phishing-Mails genutzt werden, ohne Wissen der Besitzer. So werden die kriminellen Machenschaften unter falschem Namen getätigt.

Pascal Lamia: Bedrohung aus dem Netz.

DDoS

Ein DDoS ist wie ein überfüllter Briefkasten, alle schicken eine Anfrage an den Rechner, bis er überlastet ist. Wird die Überlastung von einer grösseren Anzahl anderer Systeme verursacht, ist das ein Distributed Denial of Service (DDoS), ein verteilter Angriff.

Lamia: «Sie erinnern sich, ein Schweizer Finanzinstitut sperrt Konten von Wikileaks-Gründer Julien Assange. Von Wikileaks-Sympathisanten wurde umgehend eine Kampagne lanciert und das Finanzinstitut war per Internet nicht mehr erreichbar.»

Heartbleed

Diese Sicherheitslücke ist nicht kriminellen Ursprungs, sondern eine Lücke, die bei der Programmierung übersehen worden ist. Sie existiert seit zwei Jahren in den Bereichen der OpenSSL-Programme.

Hier konnte die Empfehlung von MELANI umgesetzt werden, die Systeme innerhalb max. 48 h zu patchen, also die korrigierte Programmversion zu laden. Gefahr erkannt, Gefahr gebannt; aber in welchem Programm steckt der nächste Fehler?

Skimming

Vor einigen Jahren wurden in der Schweiz Bankomaten von Kriminellen so umgebaut, dass die Daten der Magnetstreifen von Kreditkarten oder Bankkarten ausgelesen werden konnten. In einer Aktion können so innert weniger Minuten grosse Summen abgehoben werden.

Malware

Beispiel einer Malware: Sie erhalten ein Spam mit Attachment. Durch das Öffnen des Anhanges, kann Bild oder Text sein, beginnt die Installation der Malware, der Trojaner wird geladen. Die Malware klinkt sich in den Browser ein, sobald wir mit *online banking* beginnen.

Vhishing (Voice phishing)

Geschultes Personal, meistens in der Landessprache, ruft Computerbesitzer an und erzählt von «nötigen Updates» und «Sicherheitslücken», für die sie eine Lösung hätten. Mittels Fernwartungsprogrammen erhalten sie so oft Zugang zum Rechner und kopieren Passwörter und Rechnerdaten.

Ransomware (Einschüchterung)

«Der Zugang zu Ihrem Computer wurde gesperrt.» Diese Meldung auf dem Bildschirm lässt den Puls höher schlagen. Abhilfe soll dann eine Zahlung von 50 bis 200 Franken auf ein Konto schaffen.

Fazit: Kampf im Netz

Informationstechnologie ist allgegenwärtig und ein wichtiger Bestandteil im Daily Business vieler Unternehmen. Sie bietet neue Möglichkeiten, aber auch neue Verletzbarkeiten. Das organisierte Verbrechen verfügt über hervorragende Mittel und setzt diese gewinnbringend ein. Angegriffen wird im Moment alles, was Geld bringt und/oder einen Informationsvorsprung (Know-how-Gewinn zum Nulltarif).

Wichtiger Hinweis

Auf *www.melani.admin.ch* finden Interessierte aktuelle Hinweise auf Bedrohungen aus dem Internet und empfehlenswerten Schutz. MELANI analysiert, informiert, sensibilisiert und richtet sich speziell an private Internetbenutzer sowie an KMUs.