Da ist der Wurm drin

In Zukunft reden wir nicht mehr nur über die Dicke der Betonhülle eines Atomkraftwerkes, wenn es um Sicherheit geht, sondern darüber, wie Cyberangriffe auf Industrieanlagen abgewehrt werden können: Geheimdienste und Terroristen rüsten digital auf und schicken statt Bomben Viren und Würmer auf die Reise

Text: Astrid Herbold

→ Jedes Jahr treffen sich in Tallinn, der Hauptstadt von Estland, etwa 70 Männer und Frauen zu einer militärischen Übung. Sie sitzen dazu ganz zivilisiert in einem Konferenzraum und tippen auf Laptops. Auch die Arbeitszeiten sind moderat. Von 9 bis 18 Uhr dauern Angriff und Verteidigung, danach ist Feierabend. Trotzdem – das Ganze ist ein Kriegsspiel. „Es geht darum, Verteidigungsstrategien zu erproben und die Kooperation in multinationalen Teams zu üben“, erklärt Kristiina Pennar, eine der Organisatorinnen.

Pennar arbeitet beim CCD COE, dem Nato Cooperative Cyber Defence Centre of Excellence. Der Name ist lang, das Institut klein. 2008 wurde das Cyberabwehr-Zentrum gegründet, seitdem richten hier 35 Mitarbeiter Praxisseminare und Konferenzen aus und veröffentlichen Bücher. „Wir sind nicht dazu da, Europa zu verteidigen“, erklärt Pennar. „Wir sind eher ein Thinktank. Wir trainieren IT-Experten und betreiben Forschung.“

Beides scheint bitter nötig. Denn Cyberattacken sind längst keine düsteren Zukunftsvisionen mehr. Alle paar Wochen macht die Entdeckung neuer Superwürmer international Schlagzeilen. Geheime Dateien auf den Servern von russischen und asiatischen Regierungen, Militär- und Forschungseinrichtungen – über Jahre hinweg von einem Wurm namens „Red October“ systematisch ausgelesen und kopiert. Das Redaktionssystem der „New York Times“ – vermutlich von China aus gehackt. Zehntausende Computer der staatlichen Ölgesellschaft in Saudi-Arabien – geentert und ausgeschaltet. Eine Uran-Anreicherungsanlage im Iran – gefährlich manipuliert mithilfe des Wurms „Stuxnet“. Und die Liste ließe sich fortsetzen.

> Es ist schwer zu erkennen, wer einen da eigentlich angreift

„Wir beobachten durchschnittlich 150 gezielte Angriffe täglich auf Unternehmen und Institutionen weltweit“, erklärt Candid Wüest, der in Zürich als Sicherheitsexperte bei Symantec arbeitet. Das Software-Unternehmen hat sich auf die Bekämpfung von Schadprogrammen spezialisiert. Dabei sind die Zeiten vorbei, in denen sich Computerviren wie gigantische Grippewellen über den Globus ausbreiteten. Heute bekommt buchstäblich jedes Opfer seinen eigenen, individuell konfektionierten Wurm. Baukästen dazu gibt es in illegalen Foren im Internet. Und auch das Einschleusen wird geschickt eingefädelt: „Oft bekommen ganz bestimmte Personen in einem Unternehmen eine E-Mail mit einem Trojaner im Anhang.“ Die Anschreiben sind ordentlich formuliert, inhaltlich plausibel, thematisch interessant. Die Absender recherchieren genau, welchen Köder sie verwenden müssen. Bei „Red October“ waren es Anzeigen für günstige Diplomatenwagen, zum Beispiel ein Mazda von 1998 für 2.700 Dollar.

Einen Klick später ist der Wurm bereits in den Computer eingedrungen. Und setzt von hier aus seine Reise fort. Dazu errichtet er zunächst ein Basislager, ein sogenanntes Rootkit, von dem aus er unerkannt weiter operieren kann. Oft wird dann weitere Software über das Internet nachgeladen, selten – wie bei „Stuxnet“ – führt der Wurm schon seine komplette Werkzeugkiste mit sich. Zu der üblichen Vorgehensweise eines Wurms gehört auch die Installation eines geheimen Zugangs, genannt Backdoor, über den man von außen unbemerkt in den befallenen Computer eindringen und ihn weiter zweckentfremden kann, zum Beispiel als Spamschleuder.

Um Spam geht es bei den höher entwickelten Würmern allerdings fast nie – sondern meistens um Spionage oder Sabotage. Selbst wenn das Schadprogramm später auf Hunderten Rechnern nachgewiesen wird, ist das oft nur ein Kollateralschaden. Auf Computern oder in Netzwerken, für die sie sich nicht interessieren, bleiben die Eindringlinge harmlos. „Würmer sammeln in der Regel erst einmal Informationen über das sie umgebende System. Erst wenn sie genau dort sind, wo sie hinwollen, werden weitere Module nachgeladen“, so Wüest. Das passiere zum Teil automatisch, zum Teil auch manuell.

Nur wer ist das? Der E-Mails mit Trojanern schreibt, Würmer fernsteuert, die erbeuteten Daten auswertet oder Industrieanlagen manipuliert? Um viele Cyberattacken ranken sich Mutmaßungen und Verschwörungstheorien. Als 2007 in Estland Teile des Internets zusammenbrachen und Webseiten von Banken, Regierungsbehörden und Medien tagelang nicht erreichbar waren, verdächtigte man zunächst die russische Regierung. Schnell lag das Wort Cyberwar in der Luft, die Nato schaltete sogar Sicherheitsspezialisten ein. Später stellte sich heraus, dass der Angriff relativ dilettantisch ausgeführt worden war, vermutlich steckten russische Nationalisten dahinter.

Die Würmer sind so teuer, dass sich das fast nur Staaten leisten können

Anders bei „Red October“, „Stuxnet“ oder „Flame“, einem Spionageprogramm, das 2012 auf Computern im Nahen Osten nachgewiesen wurde. Diese Würmer beeindruckten die Analysten durch ihre extrem komplexe Funktionsweise. Schnell wurde angenommen, dass hier monatelang hochspezialisierte Teams von Informatikern und Ingenieuren an der Arbeit gewesen sein müssen. Die Kosten für die Entwicklung werden auf mehrere Millionen Euro geschätzt. Summen, die sich weniger Kriminelle, sondern eher Regierungen und deren Militärs und Geheimdienste leisten können. Bei „Red October“ gibt es Hinweise auf eine chinesisch-russische Urheberschaft, noch sind das aber nur Vermutungen. Bei „Stuxnet“ und „Flame“ dagegen hat sich der Verdacht weitgehend bestätigt, dass die USA und Israel die Auftraggeber waren.

Dazu passt, dass in Washington ohnehin die Ausweitung der digitalen Kampfzone vorangetrieben wird. Laut US-Medien stockt das Pentagon seine Cyberstreitkräfte in den nächsten Jahren von zurzeit 900 auf knapp 5.000 Netzsoldaten auf. Auch in der deutschen Hackerszene weiß man davon. „Die kaufen gerade für sehr viel Geld gute Köpfe ein“, sagt ein Insider. Friedensnobelpreisträger Barack Obama befürwortet den Kurs, der US-Präsident hat im Herbst 2012 einen nichtöffentlichen Erlass unterzeichnet, der dem amerikanischen Militär auch Angriffe auf fremde Computernetze erlaubt.

In Europa sehen viele Experten diese Entwicklung kritisch. Zwar hat auch die EU-Kommission gerade eine Richtlinie für mehr Cybersicherheit vorgestellt, darin geht es aber vor allem um eine erweiterte Meldepflicht für Cyberzwischenfälle. Werden Infrastrukturbetriebe wie Wasserwerke, Energieversorger, Finanzdienste oder Serviceanbieter im Internet (zum Beispiel Suchmaschinen oder soziale Netzwerke) gezielt angegriffen, ausgespäht oder sabotiert, so sollen sie künftig staatliche Sicherheitsbehörden benachrichtigen müssen – damit die gegebenenfalls einschreiten können. Vertuschung aus Angst vor Imageschäden wäre dann verboten.

Zugleich warnte Neelie Kroes, Vizepräsidentin der EU-Kommission, aber auch vor einem globalen Wettrüsten. Auf Twitter schrieb sie an ihre knapp 62.000 Follower: „We want a peaceful strategy because you don’t want to play w/ fire by developing cyberweapons.“ Der Schweizer Candid Wüest findet digitale Vergeltungsschläge, wie sie die USA ihren Feinden mittlerweile pauschal androhen, problematisch. „Auch wenn es aussieht, als käme eine Attacke von Servern eines bestimmten Landes, muss das nicht stimmen.“ Im Internet kann man nie ganz sicher sein, wer der Gegner ist. Außer man sitzt in Tallinn, am Finnischen Meerbusen. Da sind die Bösen im roten Team und die Guten im blauen. ←

In so einen Wurm passt eine Menge rein. Und was er nicht mit sich führt, das lädt er sich im Internet runter