DuD
Datenschutz und Datensicherheit

Computer Emergency Response Team (CERT)

Dirk Fox

Gateway (Tor, Durchgang) ist ein Vermittlungscomputer, der zwei unterschiedliche, aber gleichartige Kommunikationssysteme verbindet. Dazu setzt er die Kommunikationsregeln (Protokolle) des einen in die des anderen um. So ermöglicht er den Teilnehmern beider Systeme, sich zu verständigen. In unserem „Gateway" werden Juristen technische und Technikern juristische Begriffe erläutert.

Legendär ist der erste Internet-Wurm, der im November 1988 mehr als 2.000 über das Arpanet (den Vorgänger des Internet) verbundene Unix-Rechner befiel und dort einen mehrtägigen Totalausfall verursachte.[1] Er nutzte schon länger bekannte Fehler in älteren Versionen der Unix-Programme sendmail und finger, um sich zu verbreiten.[2]

Die durch diesen Wurm verursachten Schäden hätten vermieden werden können, wenn in allen betroffenen Rechenzentren die Information über die sicherheitsrelevanten Fehler in sendmail und finger bekannt gewesen und frühzeitig durch fehlerfreie Versionen korrigiert worden wären.

Diese Erkenntnis führte Ende 1988 zur Gründung des ersten „Computer Emergency Response Teams" (CERT) an der Carnegie Mellon University in Pittsburgh. Diesem Vorbild folgten weitere amerikanische Rechenzentren und gründeten ähnliche Computer-Notfall-Teams, die sich zur Koordination und engeren Zusammenarbeit zum „Forum of Incident Response and Security Teams" (FIRST) mit heute mehr als 100 Mitgliedern (darunter viele aus Europa) zusammenschlossen.

Eine der Hauptaufgaben von CERTs ist, durch möglichst frühzeitige Benachrichtigung von IT-Verantwortlichen Bedrohungen durch gezieltes Hacking unter Ausnutzung von Fehlern in Protokollen oder Betriebssystemimplementierungen abzuwenden. Dazu analysieren sie Sicherheitsvorfälle, die ihnen gemeldet werden, und tauschen gewonnene Erkenntnisse untereinander aus. Über Informations-Bulletins zu ausgewählten Themen, Sicherheits-Bulletins und Alarmierungen („Advisories") werden die konsolidierten Ergebnisse veröffentlicht – üblicherweise in enger Kooperation mit den betroffenen Herstellern, um möglichst kurzfristig Empfehlungen für Abhilfemaßnahmen (Konfigurationshinweise, Installation eines Software-Patches oder -Updates) geben zu können.

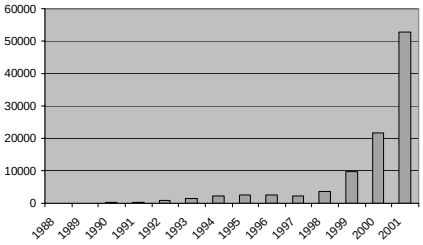

Abb.: Gemeldete Vorfälle (Quelle: CERT/CC, Carnegie Mellon)

Mit Fachkonferenzen wie dem 1989 als „FIRST-Workshop" in Pittsburgh initiierten jährlichen „Computer Security Incident Handling Workshop" (CSIHW) und dem DFN-CERT-Workshop sowie Mailinglisten wurden außerdem Foren zur Diskussion und Verbreitung von Forschungsergebnissen in diesem Gebiet geschaffen.

CERTs gehören damit heute zu den wichtigsten Informationsquellen für Erkenntnisse über Sicherheitslücken, verlässliche Informationen über aktuelle Angriffsarten und -ereignisse sowie solide Empfehlungen für Sicherheitsvorkehrungen. In Deutschland sind vor allem drei öffentliche CERT-Einrichtungen zu nennen:

- Seit 1993 bietet das Bundesamt für Sicherheit in der Informationstechnik (BSI) einen CERT-Service für Bundesbehörden an (CERT-Bund, vormals BSI-CERT).
- Ebenfalls 1993 gründete das Deutsche Forschungsnetz e.V. (DFN) ein CERT in Hamburg (DFN-CERT), das u.a. für die im WiN zusammengeschlossenen deutschen Wissenschaftsnetze (Hochschulen, Forschungseinrichtungen) zuständig ist.
- Ein drittes öffentliches CERT wird am Rechenzentrum der Universität Stuttgart (RUS-CERT) betrieben.

Verschiedene Unternehmen bieten auch kommerzielle CERT-Dienstleistungen an. Daneben werden eine Anzahl unternehmensinterner CERTs betrieben, so z.B. beim Kompetenzzentrum für IT-Sicherheit der Sparkassen-Finanzgruppe (S-CERT), der Siemens AG (Siemens-CERT) und der Deutschen Telekom AG (Telekom-CERT); weitere sind derzeit in Planung oder im Aufbau.

Für kleine und mittelständische Unternehmen plant der Bundesverband Informationswirtschaft, Telekom und neue Medien (BITKOM) die Einrichtung eines Mcert genannten Notfallteams.

Kostenlose Informationen über Sicherheitsvorfälle (Alarmierung per E-Mail) bieten u.a. auch die Firma Information Security Systems (ISS) und das System Administration, Networking and Security Institute (SANS).

Die internationale Koordination der CERT-Aktivitäten liegt heute beim CERT Coordination Center (CERT/CC) an der Carnegie Mellon University in Pittsburgh, USA, das eine sehr umfangreiche, informative und aktuelle Webseite pflegt.

CERT-Links

- CERT-Bund: http://www.bsi.de/certbund/
- CERT/CC: http://www.cert.org/
- DFN-CERT: http://www.dfn-cert.de/
- FIRST: http://www.first.org/
- ISS: http://www.iss.net/
- RUS-CERT: http://cert.uni-stuttgart.de/
- S-CERT: http://www.s-cert.de/
- SANS: http://www.sans.org/

[1] Autor des Wurms war pikanter Weise der Sohn des wissenschaftlichen Leiters des National Computer Security Centers der NSA.

[2] Eine eindrucksvolle Beschreibung dieses Angriffs findet sich im Epilog von Clifford Stolls lesenswertem Buch „Kuckucksei" (Original: „The Cuckoo's Egg", 1989).