Freiwillige Feuerwehr im Datennetz: DAS ACONET-CERT

Das Thema „Sicherheit im Internet“ wird immer brisanter – Viren, Würmer, Spam und Hacker sind allgegenwärtig und werden mit einer Unzahl technischer Hilfsmittel (Firewalls, Virenscanner und vieles andere mehr) bekämpft. Viele Firmen bieten mittlerweile umfassende Sicherheitslösungen an. Ein Aspekt wird in der Regel aber übersehen: Die technische Ebene der Internet-Security ist nur ein Teil der Wahrheit (wenn auch der, der sich leichter verkaufen lässt). Mindestens genauso wichtig ist eine Infrastruktur, die es ermöglicht, einerseits sicherheitsrelevante Informationen so früh wie möglich zu erhalten und andererseits im Ernstfall rasch und effizient zu reagieren.

Manche Netzwerkspezialisten (vor allem aus dem akademischen Bereich) haben diese Notwendigkeit schon sehr früh erkannt: Bereits im Dezember 1988 – zu einer Zeit, als das Internet noch wenig verbreitet war und Jahre, bevor das WWW erfunden wurde – entstand an der Carnegie Mellon University in Pittsburgh das CERT/CC (*Computer Emergency Response Team / Coordination Center*; siehe `http://www.cert.org/about/1988press-rel.html`) als Vorläufer und Vorbild einer stetig wachsenden Zahl von Security-Teams.

Seit 1993 gibt es auch eine weltweite Dachorganisation für CERTs: das *Forum of Incident Response and Security Teams* (FIRST). Unter den 20 Gründungsmitgliedern von FIRST befanden sich auch drei europäische Teams, allesamt aus dem akademischen Umfeld.

Security-Initiativen in Österreich

ARGE-Secure

In Österreich wurde im Jahr 2000 die ARGE-Secure gegründet, eine Arbeitsgemeinschaft von Security-Verantwortlichen heimischer Universitäten, die sich zum Ziel gesetzt hat, die nationale Kooperation und Kommunikation in Security-Fragen zu verbessern und für das österreichische Wissenschaftsnetz ACOnet die Funktionen eines CERT zu erfüllen.

Die wichtigsten davon sind *Incident Handling und Incident Response*: Bei sicherheitsrelevanten Netzwerkproblemen in seinem Zuständigkeitsbereich (*Constituency*) ist es Aufgabe des CERT, die entsprechenden Maßnahmen zu koordinieren. In den meisten Fällen bedeutet das, Beschwerden von außen an die Betroffenen weiterzuleiten und diese bei der Lösung ihres Netzwerkproblems so weit wie möglich zu unterstützen. Wenn jemand aus dem Constituency in Schwierigkeiten steckt (beispielsweise durch einen Angriff von außen), hilft das CERT natürlich ebenfalls, die Probleme zu beseitigen und die Kommunikation mit den Verursachern abzuwickeln. Neben dieser Kernaufgabe kann sich ein CERT noch vielen weiteren Tätigkeitsfeldern widmen – beispielsweise Schulungen, Publizieren von Advisories und Warnungen, Forschung oder Produkt-Evaluation (eine umfassende Dokumentation der Aufgaben eines CERT finden Sie unter dem URL `http://www.cert.org/archive/pdf/csirt-handbook.pdf`).

ACOnet-CERT

Die ARGE-Secure hat leider ein gravierendes Handicap: Für eine lose Arbeitsgemeinschaft ohne formelle Verbindungen zu internationalen Organisationen ist es schwierig, rechtzeitig an relevante Informationen zu kommen. Sicherheitsprobleme im Internet haben in der Regel globalen Charakter, und eine entsprechende Einbindung in internationale Strukturen ist unumgänglich, wenn man im Ernstfall rasch und effizient eingreifen will. Daher wurde im Jänner 2003 ein offizielles Security-Team für das österreichische Wissenschaftsnetz gegründet: das ACOnet-CERT.

Neben der oben beschriebenen *Incident Coordination*, die weiterhin überwiegend im Rahmen der ARGE-Secure abgewickelt wird, ist die wichtigste Aufgabe des ACOnet-CERT der ständige Informationsaustausch mit anderen Security-Teams. Zu diesem Zweck ist das ACOnet-CERT Mitglied von FIRST und TF-CSIRT (siehe Kasten *Internationale Security-Bündnisse* auf Seite 29). Diese Infra-

struktur bietet die Möglichkeit, einer drohenden Gefahr bereits vorbeugend entgegenzuwirken („proaktives Handeln"): Da die meisten Sicherheitsprobleme nicht in Österreich ihren Ausgang nehmen, bleibt durch die Vorab-Informationen der internationalen Partner erheblich mehr Zeit zu reagieren. Zwischenfälle, die dennoch die EndanwenderInnen erreichen (z.B. Viren, deren Verbreitungsgeschwindigkeit mittlerweile im Minutenbereich liegt), können schneller, gezielter, mit mehr Know-How und besserer Schadensbegrenzung bekämpft werden („reaktives Handeln").

Darüber hinaus bietet das ACOnet-CERT einen zentralen *Point of Contact* für Security-Fragen im ACOnet: Bei Problemen kontaktiert das CERT die Verantwortlichen der jeweiligen Teilnetze und ermöglicht ihnen dadurch ein rasches Reagieren.

Das Team des ACOnet-CERT besteht derzeit aus sieben Mitarbeitern des ZID der Universität Wien, die sich neben ihren eigentlichen Aufgabenbereichen auch mit Fragen der Security beschäftigen und das *Incident Handling* abwickeln. Da das Spezialwissen der einzelnen Team-Mitglieder praktisch jederzeit schnell verfügbar ist, erlaubt dieses System eine besonders effiziente Bearbeitung der Vorfälle.

Nähere Informationen zum ACOnet-CERT finden Sie auf der Webseite **`https://cert.aco.net/`**; für weitere Fragen steht das CERT-Team unter der Mailadresse `cert@aco.net` zur Verfügung (Tel.: +43 1 4277-14045, Fax: +43 1 4277-9140).

CIRCA

Ein weiteres österreichisches Security-Projekt, das vor allem auf eine verstärkte Kooperation der kommerziellen Internet-Provider (ISPs) in Sicherheitsfragen abzielt, ist CIRCA (*Computer Incident Response Coordination Austria*, siehe dazu auch `http://www.circa.at/`). Das Projekt CIRCA wurde im Oktober letzten Jahres von der ISPA, dem Dachverband der österreichischen Internet-Provider, ins Leben gerufen und ist unter anderem auch als Schnittstelle zwischen ISPs und Security-Firmen einerseits und dem öffentlichen Bereich andererseits gedacht.

Abgesehen von den drei vorgestellten Initiativen ist Österreich, was die Security-Infrastruktur anbelangt, leider immer noch ein eher unbeschriebenes Blatt. Es bleibt zu hoffen, dass die vorhandenen Ressourcen dennoch ausreichend sind, um den zunehmenden Gefahren aus den Weiten des Internet auch in Zukunft angemessen entgegentreten zu können.

Ulrich Kiermayr ■

Internationale Security-Bündnisse

FIRST

Das *Forum of Incident Response and Security Teams* (`http://www.first.org/`) wurde 1993 als internationale Dachorganisation für Security-Teams gegründet. FIRST hat mittlerweile etwa 150 Mitglieder aus allen Bereichen der Informationstechnologie – Softwarehersteller (z.B. *Microsoft Product Support Services Security Team*) genauso wie Hardwarehersteller (z.B. *Cisco PSIRT*), Teams aus dem Finanzwesen (z.B. *VISA-CIRT*) genauso wie nationale CERTs. Das ACOnet-CERT ist seit April 2003 FIRST-Mitglied.

Der Informationsaustausch findet bei FIRST – wie in diesen Kreisen üblich – hauptsächlich über eine Mailingliste statt, die nur für Mitglieder zugänglich ist. So kann weitestgehend vermieden werden, dass vertrauliche Hinweise zu früh an die Öffentlichkeit gelangen und der Informationsvorsprung verloren geht. Zusätzlich veranstaltet FIRST einmal jährlich eine Konferenz und zweimal jährlich ein *Technical Colloquium*, die das gegenseitige Vertrauen und den persönlichen Wissensaustausch unter den Mitgliedern fördern sollen.

TF-CSIRT

Um die Kontakte der europäischen Security-Fachleute untereinander zu verbessern, wurde 1999 eine *Task Force* der TERENA (*Trans European Research and Education Network Association*; siehe `http://www.terena.nl/`) ins Leben gerufen, die sich mit Security-Fragen befasst und die entsprechenden Aktivitäten in Europa koordiniert. Die TF-CSIRT (*Task Force – Collaboration of Security Incident Response Teams*) richtete sich anfänglich eher an die Wissenschaftsnetze, hat sich aber mittlerweile zu einem Forum für europäische CERTs aus allen Bereichen entwickelt.

Unter den zahlreichen Projekten der TF-CSIRT ist der so genannte *Trusted Introducer* (TI; siehe `http://www.ti.terena.nl/`) wohl das wichtigste: Dabei handelt es sich um eine unabhängige Stelle, die CERTs auf der Basis formaler Kriterien akkreditiert. Indem der Trusted Introducer einen gewissen Mindeststandard in Bezug auf Arbeitsweise und Dokumentation der „beglaubigten" Security-Teams sicherstellt und die Informationen über die einzelnen Teams auf dem aktuellen Stand hält, entsteht ein schlagkräftiges *Web of Trust*, dessen Mitglieder auch ohne aufwendige wechselseitige Beziehungen im Ernstfall rasch gemeinsam vorgehen können. Darüber hinaus unterhält die TF-CSIRT auch gute Kontakte zur Europäischen Kommission, sodass in den letzten Jahren im Security-Bereich eine ganze Reihe von EU-geförderten Projekten verwirklicht werden konnte.

ACOnet war in der TF-CSIRT von Anfang an sehr aktiv; das ACOnet-CERT wurde dann im März 2003 durch den *Trusted Introducer* auch formal akkreditiert.