Praktische Hilfe bei Sicherheitsvorfällen – Ein neues RIPE-Objekt

Marco Thorbrügge
DFN-CERT GmbH
Heidenkampsweg 41
D-20097 Hamburg/Germany
mailto: thorbruegge@cert.dfn.de
http://www.dfn-cert.de

Ansprechpartner und Verantwortliche für Computersysteme oder ganze Netzwerke zu finden gehört zum Tagesgeschäft eines jeden Computer-Notfallteams. In den allermeisten Fällen bedeutet dies, eine WHOIS- Abfrage in der Datenbank eines regionalen Internet Registrierungsdiensten zu starten: bei RIPE für Europa, AERIN für Nordamerika, APNIC für den asiatisch/pazifischen Raum und LACNET für Lateinamerika. Leider sind die für die Bearbeitung von Sicherheitsvorfällen notwendigen Informationen in diesen Datenbanken häufig veraltet, unkorrekt oder einfach nicht vorhanden. Abhilfe soll, zumindest für den europäischen Raum, ein neues Datenobjekt in der RIPE-Datenbank schaffen.

TRUSTED Introducer

RIPE und WHOIS

RIPE ist eine von inzwischen 4 weltweit verteilten RIR's (Regional Internet Registries) und als solche die verantwortliche Registrierungsstelle für IP-Adressen im europäischen Raum. RIPE bekommt Adressräume von IANA (Internet Assigned Number Authority) zugewiesen, und kann seinerseits wiederum Adressräume an seine Kunden, beispielsweise DE-NIC oder den DFN-Verein, deligieren. RIPE sammelt die Informationen von Personen und Einrichtungen, die IP-Adressen belegen, in einer Datenbank, der RIPE-Datenbank. Diese kann komfortabel mittels WHOIS abgefragt werden.

Mittels WHOIS lassen sich Informationen über Netzwerke und deren Betreiber ermitteln. Technische Ansprechpartner werden beispielsweise über sogenannte TECH-C Objekte verlinkt, Ansprechpartner für Abrechnungsfragen in ADMIN-C Objekten.

WHOIS und Computer Notfallteams

Das DFN-CERT ist wie jede andere Einrichtung die Incident Handling betreibt, auf die Informationen aus den Datenbanken der RIRs angewiesen, um Ansprechpartner bei Sicherheitsvorfällen zu finden. WHOIS-Abfragen lassen sich zum Einen derzeit nur bedingt automatisieren, was die Vorfallsbearbeitung erschwert. Zum Anderen stoßen das DFN-CERT und andere Notfallteams oftmals auf veraltete, unkorrekte oder fehlende Einträge mit nicht mehr gültigen Mailadressen. Ansprechpartner müssen dann mühsam von Hand gesucht werden, was die Vorfallsbearbeitung unnötig verkompliziert. Dazu kommt, dass das DFN-CERT die erste Anlaufstelle für Sicherheits- und Vorfallsfragen für die DFN-Anwender ist. Allein mit den Einträgen in der RIPE-Datenbank im derzeitigen Umfang ist es nur sehr schwer über Umwege möglich, aus einem Suchergebniss auf das DFN-CERT als zuständiges Computer-Notfallteam zu schließen.

Das RIPE-IRT Objekt

Abhilfe schaffen soll das neue IRT-Objekt, mit dessen Hilfe durch bestimmte Parameter beim WHOIS-Aufruf gleich das zuständige Notfallteam für eine IP-Adresse oder ein Netzwerk ausgegeben wird. Neben den üblichen Einträgen wie ADMIN-C oder TECH-C finden sich grundsätzliche Informationen über die Erreichbarkeit des Teams in dem Objekt: Telefon, Fax, E-Mail und Postanschrift. Darüber hinaus sind Informationen über die PGP-Keys enthalten, die für die sichere Kommunikation mit diesem Team verwendet werden können.

Verlinkt werden die IRT-Objekte mit einem INETNUM-Objekt, also dem Hauptobjekt für eine IP-Adresse bzw. einen Adressraum. Abfragbar sind diese Informationen entweder auf der RIPE-Webseite direkt oder mit dem RIPE-WHOIS-Tool und dem Parameter "-c" (auf ftp.ripe.net/tools/).

Qualitätskontrolle

Die Korrektheit und Vollständigkeit der Informationen über ein Notfallteam stellt der Service "Trusted Introducer" (TI, www.ti.terena.nl) sicher. Dieser Zertifizierungsdienst für Notfallteams übernimmt die Generierung und Aktualisierung des IRT-Objektes für Level 2 Teams wie das DFN-CERT. Dies ist sinnvoll, da der TI als vertrauensbildende Instanz immer die aktuellen Daten über ein Level 2 Team hat, denn es gehört zu den Aufgaben eines Level 2 Teams, seine Informationen in der TI-Datenbank immer aktuell zu halten. Mitarbeiter des TI haben bei der Erstellung der Spezifikationen für das IRT-Objekt sehr eng mit RIPE zusammengearbeitet und sind deshalb in der Lage, diesen Service für das DFN-CERT anzubieten.

Praktische Erwägungen

Für die Verlinkung mit einem INETNUM-Objekt eines DFN-Anwenders müssen sowohl das DFN-CERT als auch der Inhaber des INETNUM-Objektes in Form einer digitalen Signatur zustimmen. Angedacht ist, dass der DFN-Verein diese Verlinkung als Service für sämtliche INETNUM-Objekte seiner Anwender macht, für die der Verein der Maintainer ist. Genauere Informationen zum Procedere werden in den DFN-Mitteilungen sowie im DFN-Newsletter bekanntgegeben.