Automatische Warnmeldungen für Alle

Das neue DFN-CERT Portal (Teil 1)

Conficker, Mebroot & Co. machen Schlagzeilen. Damit alle Einrichtungen mit Anschluss an das X-WiN schnell darüber informiert werden, ob auch sie von diesen oder anderen Schädlingen betroffen sind, wurden die „Automatischen Warnmeldungen“ deutlich verbessert und in das neue DFN-CERT Portal integriert.

Text: **Jorgen Schäfer, Marcus Pattloch**

Das DFN-CERT ist seit vielen Jahren in der DFN-Community etabliert. Dabei werden sowohl proaktive als auch reaktive Dienstleistungen angeboten. Diese umfassen neben konkreten Hilfsmaßnahmen bei einem eingetretenen Vorfall auch zahlreiche Maßnahmen, um solche Vorfälle von Vornherein zu verhindern. Als Reaktion auf die Vielzahl neuer Bedrohungsszenarien wurden die Dienstleistungen des DFN-CERT in den vergangenen Jahren deutlich ausgebaut. Damit sich Anwender einen einfachen Überblick über aktuelle Schwachstellen und über Vorfälle, die direkt ihre Einrichtung betreffen, verschaffen können, werden Dienstleistungen des DFN-CERT nun in einer einheitlichen Oberfläche gebündelt, dem neuen DFN-CERT Portal.

Zentraler Einstiegspunkt

Das DFN-CERT Portal ist unter https://portal.cert.dfn.de erreichbar und bietet – abhängig von der Zugangsberechtigung – Zugriff auf die Dienste des DFN-CERT. Abb. 1 zeigt das allgemeine Layout des Portals. Nutzer, die bereits die DFN-PKI verwenden, werden erkennen, dass es sich eng an das Layout der Webschnittstellen der DFN-PKI anlehnt.

Über das Portal kann eine Einrichtung die DFN-CERT Dienste ihren eigenen Anforderungen entsprechend konfigurieren. Da über das DFN-CERT Portal auf sensitive Daten zugegriffen werden kann, wird besonderer Wert auf einen angemessenen Zugriffsschutz gelegt. Dieser erfolgt über Zertifikate aus der DFN-PKI Global. Greift man ohne freigeschaltetes Zertifikat auf das Portal zu, werden lediglich allgemeine Informationen wie Hilfe und Anleitungen angezeigt.

Für den zertifikatgeschützten Zugriff auf die Einrichtungsdaten benennt eine Einrichtung auf einem (papiergebundenen) Formular ihre für die DFN-CERT Dienste zuständigen Mitarbeiter. Deren Zertifikate werden dann für den Zugriff auf das Portal freigeschaltet. Damit wird sichergestellt, dass nur berechtigte Personen auf die Daten einer Einrichtung zugreifen können.

AW-Dienst im Portal

Als erster Dienst wurde der AW-Dienst (Automatische Warnmeldungen) in das Portal integriert, der in einer ersten Fassung seit Anfang 2007 verfügbar ist. Über diesen Dienst werden automatisch generierte E-Mails mit Warnmeldungen versandt, wenn beim DFN-CERT Auffälligkeiten im Zusammenhang mit IP-Adressen einer Einrichtung bekannt geworden sind. Zu diesem Zweck beobachtet und analysiert das DFN-CERT eine Reihe von Quellen, um Probleme zu entdecken, die einen Bezug zu Systemen im DFN besitzen. Darüber hinaus werden eigene Sensoren betrieben, um die Informationsbasis weiter auszudehnen. Das DFN-CERT sammelt, korreliert und normiert diese Daten und stellt jedem DFN-Anwender den Zugriff auf die Daten seiner Einrichtung zur Verfügung.

Wie wichtig der Dienst ist, zeigt die Entwicklung rund um aktuelle Schwachstellen wie Conficker oder Mebroot. Seit Ende 2008 breitet sich der Conficker-Wurm in mehreren Wellen im Internet aus. Angriffe finden von unterschiedlichen IP-Adressen auf bestimmte Ports statt. Port 445 (Microsoft-DS) ist dabei mit großem Abstand das „beliebteste“ Angriffsziel, Angriffe auf andere Ports finden kaum statt. Entsprechend dem allgemeinen An-

Abb. 1: Das DFN-CERT Portal im Überblick (Screenshot)

stieg nahm auch die an DFN-Anwender gemeldete Anzahl von Vorfällen stark zu. Wurden bis Ende 2008 ca. 10 - 20 kompromittierte Systeme pro Tag entdeckt, so hat sich diese Zahl im Frühjahr 2009 auf mehr als 100 erhöht. Insgesamt wurden über den AW-Dienst bisher mehr als 10.000 solcher kompromittierten Systeme gefunden und die Detailinformationen an die betroffenen DFN-Anwender gemeldet. Dabei handelt es sich größtenteils um Bots, Würmer und kompromittierte Rechner, die unter anderem zum Versand von Spam oder zum Ausspähen persönlicher Informationen (Zugangsdaten von Online-Banking, Webmailer, etc.) benutzt werden.

Neue Funktionen für den AW-Dienst

Mit der Integration in das DFN-CERT Portal wurde der AW-Dienst jetzt noch einmal deutlich verbessert. Eine wichtige Voraussetzung dafür war die Verknüpfung des AW-Dienstes mit der Information über die zu jeder Einrichtung zugehörigen Netzbereiche. Für alle Anwender, die ihre Netzbereiche über den DFN-Verein erhalten, liegt diese Information vor und wird im AW-Dienst aktualisiert, wenn z. B. für eine Einrichtung neue Netzbereiche dazukommen. Im Portal werden diese Netzbereiche auf Wunsch im Konfigurationsmenü angezeigt. Somit muss eine Einrichtung nicht mehr überlegen, welche einzelnen Netzbereiche zu berücksichtigen sind. Mit einer so genannten „Alles-Regel“ werden im AW-Dienst alle bekannten Netzbereiche dieser Einrichtung erfasst. Wenn Netzbereiche dazukommen oder entfallen, wird diese Änderung automatisch übernommen.

Die Übersicht über die Netzbereiche ist auch nützlich, um detaillierte Regeln zu konfigurieren. So können die Informationen zu Teilnetzen z. B. direkt einzelnen Instituten oder Abteilungen zugestellt werden. Die Konfigurationsmöglichkeiten sind dabei sehr flexibel: Netzbereiche können sowohl in CIDR-Notation angegeben werden als auch in der oft besser lesbaren „von-bis Notation“. Auch Mischformen sind möglich (Abb. 2). Die Eingabe von Netzbereichen, die nicht der Einrichtung zuzuordnen sind, wird durch die sofortige Überprüfung der Eingabedaten verhindert. Die Regeln werden – wie bei einer Firewall – immer von oben nach unten abgearbeitet. Sobald eine Übereinstimmung gefunden wird, wird diese Regel angewandt und eine entsprechende E-Mail verschickt. Dabei ist es auch möglich, mehrere Netzbereiche in einer Regel zusammenzufassen. Zudem steht eine Funktion zur Verfügung, mit der geprüft werden kann, welche Regel für einen bestimmte IP-Adressbereich greift. Dies ist besonders dann hilfreich, wenn Netzbereiche in mehreren Regeln enthalten sind.

Die für den AW-Dienst erstellten Regeln lassen sich auch als XML-Datei herunterladen, bearbeiten und wieder hochladen. Das ist z. B. nützlich, wenn bereits Informationen über die Zuständigkeiten für bestimmte Netzbereiche in eigenen Systemen vorgehalten werden. Auf Wunsch einiger Anwender wurde auch ein maschinenlesbarer Export der Vorfallsinformationen implementiert. Die verschickten E-Mails mit den Warnmeldungen enthalten nun einen XML-Anhang, in dem die Informationen aus der E-Mail noch einmal in maschinenlesbarer Form enthalten sind. Damit können die Warnmeldungen z. B. an ein internes Ticket-System zur weiteren Verarbeitung geschickt werden.

Weitere Verbesserungen des Dienstes umfassen eine Erhöhung der Anzahl der Datenquellen, detailliertere Meldungstypen (z. B. zu Conficker) und eine verbesserte Korrelation der Daten, wodurch es kaum noch zu Falschmeldungen (False Positives) kommt.

Woher kommen die Daten?

Die für den AW-Dienst verwendeten Daten stammen aus verschiedenen öffentlichen Quellen. Dabei heißt öffentlich, dass prinzipiell jeder Teilnehmer im Internet diese Daten auffangen kann. Konkret werden die meisten Informationen aus dem Betrieb von Sensoren gewonnen. Einige Sensoren lauschen auf eingehenden Verkehr in Netzblöcken, die nicht in Benutzung sind und in denen keine Dienste angeboten werden (sog. Darknets). Verbindungsversuche sollten deshalb nicht vorkommen. Werden Verbindungsversuche bzgl. eines bestimmten Dienstes zu vielen Adressen in den Netzblöcken aufgefangen, so ist dies sehr verdächtig und ein Hinweis auf ein mögliches Problem. Dies kann z. B. eine Suche nach aktiven Webservern sein, um dort bekannte Schwachstellen auszunutzen.

Andere Sensoren antworten auf Anfragen und täuschen dabei Dienste vor, in denen bekannte Schwachstellen existieren (sog. Honeypots). Kann der Sensor nun erfolgreich die Ausnutzung einer Schwachstelle vortäuschen, überträgt die Schadsoftware eine Kopie von sich selbst, um das neue Opfer zu infizieren. Die Ausführung der auf den Honeypot übertragenen Kopie wird natürlich verhindert, stattdessen wird sie von verschiedenen Scannern untersucht. Die Warnmeldung an die Teilnehmer des Dienstes, in deren Netzwerk das angreifende System steht, enthält dadurch zusätzliche wertvolle Hinweise, wie den Namen der wahrscheinlich vorliegenden Schadsoftware.

Wie kann man das DFN-CERT Portal nutzen?

Die Nutzung des DFN-CERT Portals ist für alle DFN-Anwender unentgeltlich möglich. Eine Einrichtung muss dem DFN-Verein lediglich eine so genannte „Handlungsberechtigte Person“ benennen, die im Besitz eines Zertifikats der DFN-PKI Global sein muss. Dieses Zertifikat wird dann für den jeweiligen Dienst freigeschaltet, so dass die handlungsberechtigte Person auf die Daten ihrer Einrichtung Zugriff hat.

Da die Sicherheit des gesamten Wissenschaftsnetzes erhöht werden kann, wenn möglichst viele Anwender über ihre Vorfälle informiert sind, wurde der Einstieg in den AW-Dienst jetzt wesentlich erleichtert. Nach vorheriger Rücksprache mit den Ansprechpartnern der DFN-Anwender wird der AW-Dienst in einer Basiskonfiguration mit aktivierter „Alles-Regel“ eingerichtet (Abb. 3). Die Ansprechpartner erhalten dann ab sofort die entsprechenden Warnmeldungen. Einrichtungen, die den AW-Dienst schon länger nutzen, wurden mit ihren bestehenden Regeln und freigeschalteten Zertifikaten in das DFN-CERT Portal migriert, so dass die Daten nun bei Bedarf von den handlungsberechtigten Personen über diesen Zugang bearbeitet werden können.

Ein Blick nach vorne

Mit der Integration neuer Dienste und der Ergänzung bestehender Dienste um weitere nützliche Funktionen wird das DFN-CERT Portal weiter ausgebaut.

Im nächsten Schritt wird der Advisory-Dienst, der seit vielen Jahren über neue Schwachstellen informiert, in das Portal aufgenommen. Zur Zeit erfolgt der Versand der Schwachstellen-Informationen noch über die Maillingliste „win-sec-ssc“. Das funktioniert zwar gut, jedoch haben sich mittlerweile diver-

Abb. 2: Konfigurationsbeispiel Netzbereiche mit verschiedenen Empfängern (Screenshot)

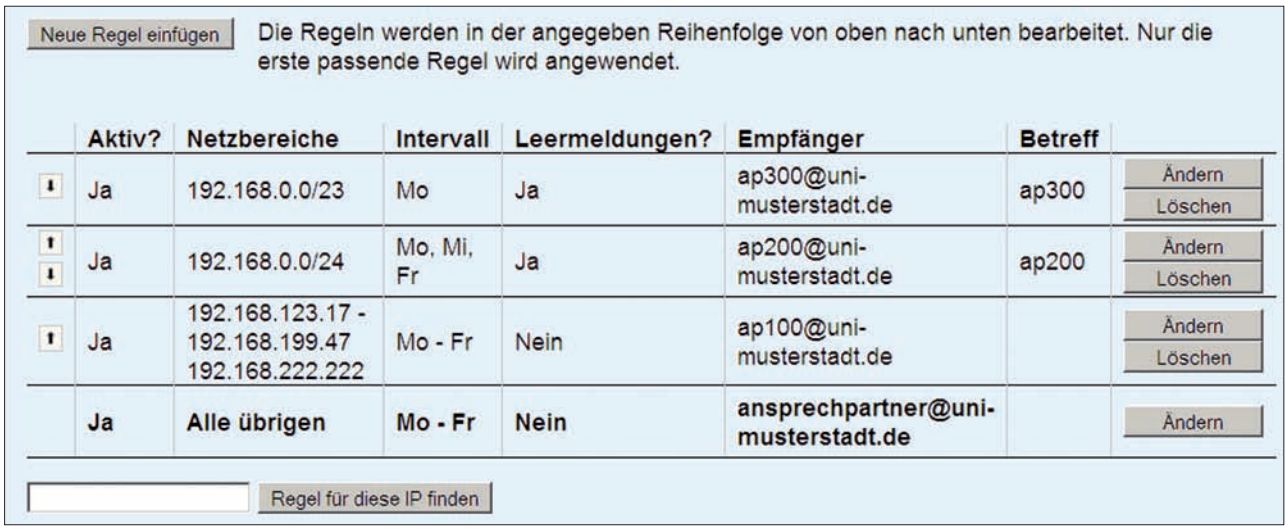

Abb. 3: Basiskonfiguration mit eingeschalteter „Alles-Regel“ (Screenshot)

se Anforderungen an Verbesserungen des Dienstes im Sinne der Nutzbarkeit und Integration in Hochschulprozesse ergeben. Im Rahmen der nächsten DFN-Betriebstagung im Oktober 2009 wird der neue Advisory-Dienst vorgestellt, in den nächsten DFN-Mitteilungen wird es einen Übersichtsartikel dazu geben. Informationen zum DFN-CERT Portal und zu den Automatischen Warnmeldungen finden Sie unter http://www.cert.dfn.de. Dort kann auch eine detaillierte Beschreibung zur Nutzung des Portals und zur Konfiguration des AW-Dienstes heruntergeladen werden. Bei Rückfragen wenden Sie sich bitte an: cert@dfn.de. ◆

Der sichere Zugriff auf das DFN-CERT Portal

Der Zugriff auf die Warnmeldungen einer Einrichtung darf nicht durch Unbefugte erfolgen. Zu diesem Zweck setzt des DFN-CERT Portal an jeder Stelle auf verschlüsselte Datenverbindungen über SSL, X.509 und Zertifikate der Global-Hierarchie der DFN-PKI. Dies beinhaltet auch die internen Verbindungen, die vollständig hinter Firewalls ablaufen.

Dabei gibt es einige Herausforderungen. Jedes Zertifikat muss nicht nur gegen die mehr als 200 Zertifizierungsstellen der DFN-PKI Global geprüft werden, zusätzlich müssen auch die mehr als 200 zugehörigen Certificate Revocation Lists (CRLs) einer Prüfung unterzogen werden. Das Modul mod_ssl des Apache Webservers ist hierfür nur bedingt geeignet, da regelmäßig neue Einrichtungen an der DFN-PKI teilnehmen und die CRLs an unterschiedlichen Stellen auf aktuellem Stand gehalten werden müssen. Weiterhin lässt sich eine feingliedrige Zugriffskontrolle für die erlaubten Zertifikate mit dem Apache-Modul nur sehr umständlich realisieren.

Daher verwendet das DFN-CERT Portal für die Bearbeitung der verschiedenen Aufgaben eine selbst geschriebene Software namens certval. Die Software lädt automatisiert CRLs von den jeweiligen CRL-Servern nach und hält diese einige Zeit vor, um eine hohe Abarbeitungsgeschwindigkeit zu ermöglichen. Welche Zugriffsrechte für einen Nutzer freigeschaltet sind, wird unter dem Menüpunkt „Nutzerinformationen“ im „Hilfe“-Reiter angezeigt. ◆