Informationen zu Schwachstellen

Das neue DFN-CERT Portal (Teil 2)

Text: **Gerti Foest** (DFN-Verein), **Torsten Voss** (DFN-Cert Services GmbH)

Foto: © moodboard, fotolia

Sicherheitslücken in Betriebssystemen und Anwendersoftware treten immer wieder auf. Nur rechtzeitige Information ermöglicht es Nutzern und Administratoren, notwendige Maßnahmen zu ergreifen, um die Ausnutzung solcher „Schwachstellen“ zu verhindern. Über das DFN-CERT Portal kann man sich nun gezielt über Schwachstellen in genau den Systemen informieren lassen, die in der eigenen Arbeitsumgebung relevant sind.

Seit vielen Jahren sammelt das DFN-CERT Informationen zu Schwachstellen und veröffentlicht sie angereichert mit Hintergrundinformationen als so genannte Advisories auf der Mailingliste win-secssc. Mit der Integration in das DFN-CERT Portal wurde dieser Dienst nun deutlich verbessert. Je nach Zugangsberechtigung stehen über das Portal verschiedene Möglichkeiten für die Nutzung zur Verfügung: Von der Recherche im neu eingerichteten Archiv bis zur individuellen Konfiguration eines Abonnements der Informationen zu Schwachstellen.

Der neue Dienst im DFN-CERT Portal

Im DFN-CERT Portal stehen unter https://portal.cert.dfn.de jetzt neben den „Automatischen Warnmeldungen“ (DFN-Mitteilungen Heft 76, S. 44 ff.) auch die Informa-

tionen zu Schwachstellen zur Verfügung. Welche Möglichkeiten für alle Nutzer zur Verfügung stehen und welche mit einem Zertifikat oder einer weiteren Zugangsberechtigung genutzt werden können, zeigt Abbildung 1.

Jeder Nutzer des Portals hat unter dem Auswahlpunkt „Archiv“ Zugriff auf alle bisher versandten Informationen zu Schwachstellen. Eine Auswahlbox ermöglicht die gezielte Suche nach Meldungen in bestimmten Systemen (z.B. Debian oder Windows) oder nach frei wählbaren Stichworten im gesamten Archiv.

Nutzt man das Portal mit einem Zertifikat der DFN-PKI Global, besteht zusätzlich die Möglichkeit, ein Abonnement der Informationen zu Schwachstellen zu konfigurieren (Abbildung 2). Unter dem Auswahlpunkt „Konfiguration“ können die Systeme, über die der Nutzer informiert werden möchte und das Format, in dem die Meldungen verschickt werden sollen, ausgewählt werden. Neue Informationen werden dann an die im Zertifikat verankerte E-Mail-Adresse geschickt. Wenn das Zertifikat mehrere E-Mail-Adressen enthält, kann die gewünschte Empfängeradresse ausgewählt werden.

Eine weitere Konfigurationsmöglichkeit steht für sogenannte handlungsberechtigte Personen (HP) zur Verfügung. Eine handlungsberechtigte Person wird von einer Einrichtung mit einem Formular für den Dienst DFN-CERT als verantwortlicher Ansprechpartner benannt. Nach Eingang des unterschriebenen Formulars wird das Zertifikat der HP für den Auswahlpunkt „Konfiguration (HP)“ im Portal freigeschaltet. Diese Funktion erlaubt neben den oben beschriebenen Konfigurationsmöglichkeiten auch das Eintragen von E-Mail-Adressen, die nicht im eigenen Zertifikat verankert sind, z. B. einer einrichtungsinternen Verteilerliste.

Kurzformat und Langformat

Aufgrund der vielen Informationen, die das DFN-CERT zu einer Schwachstelle zusammenträgt, können Schwachstellenmeldungen zum Teil sehr umfangreich werden. Oft sind aber nur wenige Hinweise notwendig, um die Relevanz einer solchen Meldung für das eigene Umfeld beurteilen zu können. Deshalb können die Informationen zu Schwachstellen nun über das DFN-CERT Portal in zwei Ausführungen bezogen werden: Im Kurz- und im Langformat.

Das Kurzformat (Abbildung 3) enthält Informationen zur betroffenen Software, den betroffenen Plattformen und eine Kurzbeschreibung, wie die Schwachstelle von einem Angreifer ausgenutzt werden kann. Hat eine Schwachstelle bereits „eine Geschichte“, wird auch diese Historie aufgeführt. Am Ende jeder Kurzmeldung steht der Verweis auf die Meldung im Langformat. Das Langformat enthält zusätzlich zu den Informationen, die auch im Kurzformat zu finden sind, Beschreibungen aller beinhalteten Schwachstellen mit ihren CVE-Nummern (Common Vulnerabilities and Exposures) sowie Verweise auf die Hersteller-Advisories und ggf. weitere Quellen mit Zusatzinformationen. Wenn vom Hersteller schon ein Update zur Verfügung gestellt wird oder ein sinnvoller Workaround bekannt ist, werden auch dazu Hinweise im Langformat gegeben.

Abb. 1: Zugriffsrechte

	Archiv	Abo-Adresse aus Zertifikat	Abo-Adresse frei wählbar
Alle Nutzer ohne Zertifikat	✓	X	X
Alle Nutzer mit Zertifikat	✓	✓	X
Handlungsber. Personen mit Zertifikat	✓	✓	✓

Woher kommen die Informationen?

Das DFN-CERT sammelt Sicherheitswarnungen von Herstellen und überprüft darüber hinaus Kanäle, auf denen Update-Informationen zur Verfügung gestellt werden. So werden z.B. im Austausch mit anderen CERTs zusätzliche Hintergrundinformationen erarbeitet, die Antworten auf folgende Fragen geben können:

- Unter welchen Voraussetzungen ist ein System betroffen?
- Wie können Angriffe auf die Schwachstelle z.B. in den Log-Daten des Systems erkannt werden?
- Wie kritisch ist die Schwachstelle und wird sie bereits in der Praxis ausgenutzt?
- Steht für das betroffene Programm ein Update bereit oder gibt es einen temporären Workaround?

Viele Hersteller verwenden für die Kennzeichnung von Schwachstellen eine standardisierte Bezeichnung, die CVE-Nummer. Taucht eine Schwachstelle in unterschiedlichen Softwareprodukten auf, kann sie dadurch eindeutig zugeordnet werden und das DFN-CERT kann diese Informationen in einer Schwachstellenmeldung bündeln. Alle verfügbaren Informationen werden vom DFN-CERT zusammengefasst, in ein einheitliches und „menschenlesbares“ Format gebracht und als Schwachstellenmeldungen an interessierte Nutzer weitergegeben.

Hintergrund: Updates und Exploits

In sensiblen Bereichen wie in der Luftfahrt oder der Medizin werden Programme vor ihrer Freigabe sehr genau geprüft, um möglichst alle Fehler zu beseitigen. Al-

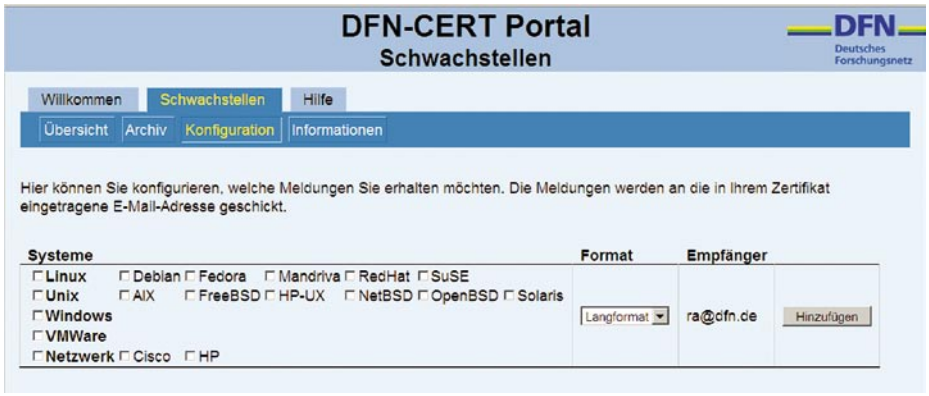

Abb. 2: Konfiguration mit Zertifikat der DFN-PKI Global

Liebe Kolleginnen und Kollegen,

bitte beachten Sie die folgende Sicherheitsmeldung.
Betroffene Software:
Paket backuppc
Betroffene Plattformen:
Mandriva Enterprise Server 5
Mandriva Enterprise Server 5/X86_64

Aufgrund einer Schwachstelle in BackupPC können am System angemeldete Benutzer ein Backup und Restore anderer Systeme vornehmen und dadurch auch Dateien dieser Systeme einsehen oder verändern.

Weitere Informationen finden sie unter:
<https://portal.cert.dfn.de/adv/DFN-CERT-2009-1385/>

Mit freundlichen Grüßen,
Ihr DFN-CERT Team

Abb. 3: Prägnantes Kurzformat einer Schwachstellenmeldung

lerdings kostet eine solche Prüfung viel Zeit und Geld und wird deshalb in weniger sensiblen Bereichen nicht immer konsequent durchgeführt. Bei „normaler“ Software rechnet man mit mindestens einem Fehler pro 1.000 Zeilen Programmcode. Wird ein solcher Fehler entdeckt, stellen die Hersteller von Betriebssystem- oder Anwendersoftware normalerweise eine berichtigte Programmversion als Update („Patch“) zur Verfügung. Nach dem Einspielen des Updates sollte der Fehler behoben sein.

Eine wichtige Frage bei der Beurteilung des Risikos einer Schwachstelle ist, ob dazu schon ein Exploit existiert. Ein Exploit ist ein Programm, mit dem eine Schwachstelle z.B. zum Eindringen in das System ausgenutzt wird. Exploits werden zum Teil frei im Internet veröffentlicht, es hat sich aber auch ein Schwarzmarkt etabliert, auf dem Exploits an interessierte Abnehmer verkauft werden. Ist ein Exploit für eine Schwachstelle bereits im Umlauf und wird vom Hersteller ein Update für diese Schwachstelle angeboten, ist grundsätzlich ein umgehendes Einspielen des Updates zu empfehlen.

Besonders gefährlich ist ein Exploit, wenn vom Hersteller der Software noch kein Update zur Verfügung gestellt wird und viele Benutzer von der Schwachstelle betroffen sind. In diesem Fall gibt es als Gegenmaßnahme nur die Möglichkeit eines Workarounds, zum Beispiel das Abschalten bestimmter Programmteile oder die Einschränkung des Zugriffs auf betroffene Software. Damit kann die Zeit bis zum Erscheinen eines Updates überbrückt und die Gefahr der Ausnutzung der Schwachstelle minimiert werden.

Zusammenfassung

Nur wenn Nutzer und Administratoren Kenntnis über Schwachstellen und ihre möglichen Folgen haben, können sie eine Entscheidung über angemessene Gegenmaßnamen fällen. Bereits seit mehreren Jahren ist die Information zu Schwachstellen ein wichtiger Dienst des DFN-CERT. So wurden alleine in den letzten 12 Monaten mehr als 2.000 Schwachstellenmeldungen veröffentlicht. Mit der Integration in das DFN-CERT Portal konnte der Dienst nun verbessert und um wichtige neue Funktionen ergänzt werden.

Info

Sie erreichen das DFN-CERT Portal unter https://portal.cert.dfn.de. Weitere Informationen und eine ausführliche Nutzungsanleitung finden Sie unter www.cert.dfn.de/schwachstellen.

Für Fragen und Anregungen zum Portal schicken Sie bitte eine E-Mail an: cert@dfn.de. ◆