Das neue DFN-CERT Portal

Das Thema IT-Sicherheit wird immer präsenter, die Anzahl an sicherheitsbezogenen Maßnahmen nimmt stetig zu und das Bedürfnis nach Schutz wächst mit jedem neuen öffentlich kommunizierten Angriff. Dadurch wächst auch der Informationsbedarf und die Anforderungen an eine effiziente zielgruppenspezifische Kommunikation von sicherheitsrelevanten Informationen steigen.

Text: **Nina Bark, Ralf Gröper** (DFN-Verein)

Das DFN-CERT bietet genau die Informationen, die für mehr Sicherheit im Internet und insbesondere für den Schutz von Rechnern und Computernetzen gebraucht werden. Dazu bündelt das DFN-CERT Sicherheits-Know-How in enger Kooperation mit deutschen und internationalen Computer Notfall-Teams. In dieser leistungsfähigen Sicherheitsinfrastruktur laufen Informationen aus aller Welt zusammen. Das DFN-CERT wurde 1993 zunächst als reines Computer-Notfallteam für die Anwender des Deutschen Forschungsnetzes ins Leben gerufen, heute ist es ein hochspezialisierter Dienstleister für mehr Sicherheit im Internet.

Eine der Hauptaufgaben des DFN-CERT ist es, die Fülle an sicherheitsrelevanten Informationen zu bewerten, zu bündeln und zu kommunizieren. Dafür stehen dem DFN-CERT verschiedene Kommunikationskanäle zur Verfügung, durch welche die verarbeiteten Informationen zu den Anwendern gelangen können.

Einer dieser Kanäle ist der DFN-CERT-Dienst und das zugehörige DFN-CERT Portal. Hier werden sicherheitsrelevante Daten aus vielen verschiedenen Quellen zusammengeführt und entsprechend ihrer Konfiguration wieder an viele Senken verteilt. Die herauszugebenden Daten lassen sich in drei Dienste unterteilen:

- Warnmeldungen,
- Schwachstellenmeldungen,
- Netzwerkprüfer.

Foto © adrian825/iStockphoto

Pro Tag werden zahlreiche Informationen an einen Anwender weitergegeben. Die Schwierigkeiten, die sich für die Verarbeitung dieser Informationsflut ergeben, liegen auf der Hand. Es wird immer schwieriger, den Überblick über die relevanten Informationen zu behalten und eine effektive Bearbeitung zu gewährleisten.

Informationsflut bändigen

Um die Fülle an Informationen der verschiedenen Dienste besser zu verzahnen und dadurch einen besseren Überblick zu schaffen, und um Verantwortungsbereiche effizienter delegieren zu können, wurde das DFN-CERT Portal komplett neu entwickelt und dabei umstrukturiert.

Durch eine feingranulare Konfiguration ist es nun möglich, genau zu definieren welche Informationen an welchen Mitarbeiter (Admin) gehen sollen. Dem DFN-Verein von den Einrichtungen benannte sogenannte handlungsberechtigte Personen (HPs) können ihr Netz im Portal modellieren und so Subnetze anlegen, für die sie lokale Ansprechpartner selber festlegen und ins Portal einladen können. Der eingetragene Ansprechpartner kann nur die für ihn relevanten Netzbereiche und Domains einsehen und kommt so direkt an die für ihn entscheidenden Informationen. Außerdem kann er die von ihm verwaltete Software definieren, um auch nur hierfür die bereitgestellten Informationen wie Schwachstellenmeldungen zu erhalten.

Durch das Definieren der einzelnen Ansprechpartner wird ein neuer effizienterer Workflow ermöglicht. Die Kontakte für jedes Subnetz bekommen die Informationen der drei Dienste speziell für ihren Bereich angepasst:

Warnmeldungen
Welche IPs aus meinem Subnetz sind auffällig geworden?

Schwachstellenmeldungen
Welche Schwachstellen hat die Software, die in meinem Subnetz läuft?

Netzwerkprüfer-Ausgaben
Welches Subnetz soll gescannt werden und welche Ergebnisse haben bereits durchgeführte Scans?

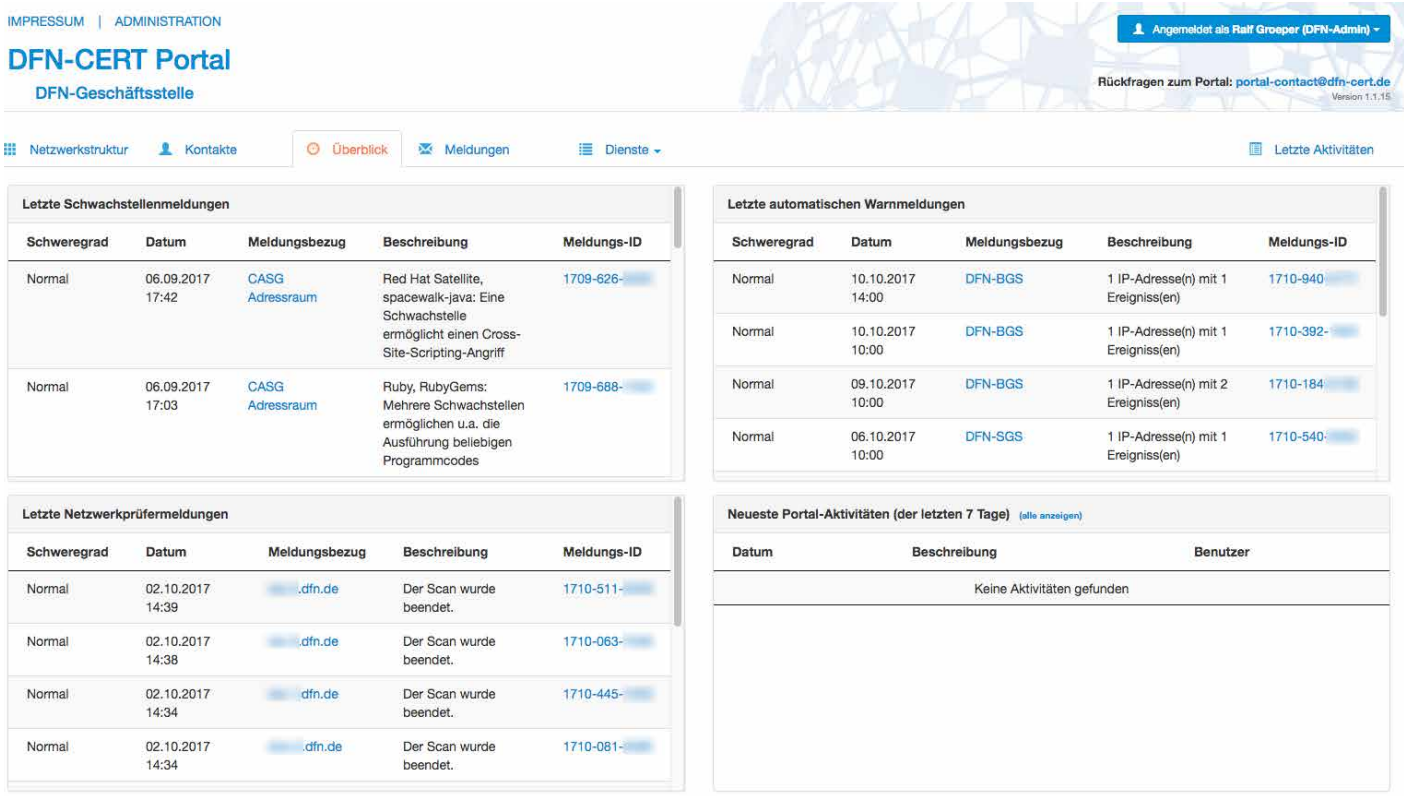
Um der Informationsflut noch besser entgegenzuwirken, werden alle Meldungen im Portal dargestellt und nur noch optional per E-Mail versandt. Auf dem Dashboard sind alle Meldungstypen auf einen Blick zu sehen, um so den Sicherheitsstatus für jedes Subnetz abrufbar zu machen. Als Neuerung werden die Ereignisse, die zweimal pro Tag als automatische Warnmeldung aggregiert ausgeliefert werden, nun zusätzlich (fast) in Echtzeit im Portal veröffentlicht.

Einheitliche Meldungen

Eine weitere Neuerung ist das Konzept der Meldungen im Allgemeinen: Diese werden einheitlich für Events aller drei Dienste dargestellt. Durch ein Filtersystem können die Meldungen dann nach Meldungstyp (Warnmeldungen, Schwachstellenmeldungen, Netzwerkprüfer-Ausgaben oder manuelle Meldungen) sortiert werden. Um auch hier noch effizienter an Informationen zu gelangen, lassen sich die Meldungen zusätzlich nach Schweregrad und Netzbereich filtern. Durch eine Volltextsuche ist es möglich, spezifische und auch nicht mehr aktuelle Meldungen schnell zu finden. Eine Kombination von Filtern kann durch einfaches Anlegen eines Bookmarks gespeichert werden, sodass verschiedene, von den Nutzern selber gestaltete Ansichten des Portals schnell aufrufbar sind, zum Beispiel für das Live-Monitoring verschiedener Aspekte des eigenen Netzes.

Die einheitlichen Meldungen werden im Portal archiviert und bieten einen zeitlichen und räumlichen Überblick. So kann z. B. schnell erfasst werden, was das DFN-CERT für einen bestimmten Netzbereich (z. B. Uni-Verwaltung) in der letzten Woche gemeldet hat.

Insgesamt erleichtert das neue DFN-CERT-Portal die Bändigung der täglichen Informationsflut zu sicherheitsrelevanten Events. Es ermöglicht, dass Informationen nur den direkt verantwortlichen Ansprechpartnern kontextbezogen angezeigt werden. Diese können sich also auf das Wesentliche konzentrieren und für den Einzelnen im aktuellen Kontext nicht relevante Meldungen werden gar nicht erst angezeigt. ◆



Beispiel Dashboard DFN-CERT Portal