

Organisation von Diensten der IT-Sicherheit

Ergänzendes Material zum Papier IT-Sicherheit an Hochschulen

Erarbeitet durch den AK-„IT-Sicherheit“ von Herbst 2004 bis Sommer 2005
Version 1.0 - Stand Oktober 2005

Die große Heterogenität der Verfahren (inkl. DV-Hardware und -Software) stellt hier das zentrale Problem dar. Für alle in der Rahmenrichtlinie erarbeiteten Gruppen gleichartiger Systeme ist ein Katalog von Einzelmaßnahmen zu formulieren, umzusetzen und aktuell zu halten. Dieser enorme Arbeitsaufwand kann in Kooperation zwischen den Rechenzentren des ZKI vorangebracht werden. Unterstützung kann von den diversen Sicherheitsforen im Internet ausgehen, wobei die spezifischen Gegebenheiten an Hochschulen dort selten Berücksichtigung finden. Die individuelle Situation vor Ort kann ausschließlich durch die lokalen Verantwortlichen für die Systeme beurteilt und entsprechende Maßnahmen umgesetzt werden. Die Rolle der lokalen, nationalen und internationalen CERTs muss hier berücksichtigt werden.

1 Organisation der Informationsdienste

Der Austausch bzw. die Weitergabe von sicherheitsrelevanten Informationen, egal ob innerhalb einer Einrichtung oder zwischen Einrichtungen, ist ein wichtiger Aspekt bei der Realisierung und Gewährleistung der IT-Sicherheit. Durch einen gut organisierten Informationsdienst kann entsprechend schnell vorbeugend (präventiv) bei Sicherheitslücken bzw. reaktiv bei Sicherheitsvorfällen gehandelt werden.

Es gibt grundlegende sicherheitsrelevante Informationen, die periodisch verbreitet werden bzw. generell öffentlich einsehbar sein sollen. Diese z.T. längerfristig gültigen und damit grundlegenden Informationen sind zum Beispiel:

- Informationen zum Umgang mit Passwörtern
- Informationen zum Virenschutz
- Informationen zum sicheren Kommunizieren (Einsatz vom PGP)
- Sicherheitsregeln für die Nutzung von PCs

Eine andere Art von sicherheitsrelevanten Informationen sind solche, die sich schneller ändern also Material über neue Sicherheitspatches, neue Viren, aktuelle Vorfälle und ähnliches. Für diese sind folgende Informationswege geeignet:

- Mailinglisten
- spezielle WWW-Seiten
- periodische Schulungen/Workshops für DV-Organisatoren und Sicherheitsbeauftragten der Bereiche einer Einrichtung

Hierbei sollte versucht werden, diese Informationswege so themenspezifisch wie möglich zu gestalten (z.B. Mailinglisten für Betriebssysteme unterteilt nach Windows, Unix bzw. Mac OS). So ist eine effektive und überschaubare Informationsweise und Nutzbarkeit gewährleistet. Eine mögliche Strukturierungen solcher Informationen werden im nächsten Abschnitt beschrieben.

Sollen sicherheitsrelevante Informationen in der eigenen Einrichtung generiert werden, muss für alle Beteiligten das entsprechende Format bekannt sein (entsprechendes Muster veröffentlichen). Dadurch ist eine effektive und schnelle Erarbeitung bzw. Bearbeitung dieser Informationen möglich. Auch externe Informationen könne vor der internen Weitergabe entsprechend dem genutzten Format aufbereitet werden. Durch die Verwendung eines standardisierten Formates wird eine Archivierung und spätere Auswertung bzw. Weiternutzung wesentlich erleichtert.

Sollten sich mehrere Einrichtungen zu ähnlichen oder gemeinsam genutzten Formaten bekennen, können durch gezielte gegenseitige Information hohe Synergieeffekte erzielt werden. Durch die Verwendung eines gemeinsamen Formats wird eine übergreifende Suche über verschiedene Kriterien (Attribute, Metadaten) möglich.

Die Sammlung der Maßnahmen und Meldungen kann an zentraler Stelle oder dezentral Bereitstellung mit zentraler Suchmöglichkeit erfolgen. In beiden Fällen muss für Nutzbarkeit dieses Informationsdienstes die Aktualität und Pflege gesichert sein. Dieser Informationsdienst kann ggf. als Kooperation innerhalb des ZKI betrieben werden.

2 IT-Sicherheitsmaßnahmen und Meldungen

Das IT-Grundschutzhandbuch des BSI enthält Standardsicherheitsmaßnahmen, Umsetzungshinweise und Hilfsmittel für zahlreiche Konstellationen, die typischerweise im Einsatz anzutreffen sind. Dieses Informationsangebot soll zur zügigen Lösung häufiger Sicherheitsprobleme dienen, die Anhebung des Sicherheitsniveaus von IT-Systemen unterstützen und die Erstellung der Rahmenrichtlinie der IT-Sicherheit vereinfachen. Die im IT-Grundschutzhandbuch zusammengestellten Standardsicherheitsmaßnahmen orientieren sich dabei an einem Schutzbedarf, der für die meisten IT-Systeme zutrifft.

Das IT-Grundschutzhandbuch ist als "weiterentwicklungsfähiges Werk" angelegt. Durch eine halbjährliche Fortschreibung sollen Verbesserungsvorschläge, Erweiterungen sowie die Weiterentwicklung der IT berücksichtigt werden.

Aufgrund der Fülle der Information (mehr als 2900 Seiten des Grundschutzhandbuchs) und der erforderlichen Zeit zur Überarbeitung müssen Meldungen (engl. Announcements) zu aktuellen Sicherheitsthemen verfasst werden. Damit die jeweilige Information schnell und zuverlässig gefunden wird, ist eine strenge Strukturierung der Meldungen sinnvoll. Das RUS-CERT hat zu diesem Zweck das Common Announcement Interchange Format (CAIF) vorgeschlagen, welches sich zu einem anerkannten Standard entwickelt hat. Dieses Format strukturiert u.a. folgende Informationen:

- Identifikation des Dokumentes
- Zielgruppen, Revisionen
- Kategorisierung der (nicht oder nur möglicherweise) betroffenen IT-Systeme
- Problemaspekte
- mögliche Maßnahmen und Workarounds

In Anhang E wird eine Übersicht der Struktur der Meldungen dargestellt. Entsprechende Meldungen beziehen sich überwiegend auf bekannte Angriffe oder offene Sicherheitslücken. Für die verschiedenen Nutzer soll eine zeitorientierte, dienstbezogene und technologiebezogene (Über-)Sicht angeboten werden. Dadurch wird ein Bezug zum Zielgruppenspektrum (Administratoren ... Endanwender) möglich.

3 Sicherheitsmanagement

Um die diversen Sicherheitsbelange adressieren zu können, ist ein Team aus technisch qualifizierten Mitarbeitern zu bilden, die sowohl tiefen Einblick in die Verwaltung komplexer Netze als auch die Administration von Endsystemen besitzen. Die Kommunikation mit den entsprechenden Abteilungen zum Betrieb der Infrastruktur muss sehr eng sein, um aktuell auftretende Schwachstellen und andere Bedrohungen rasch und fundiert bewerten zu können.

Neben der Bewertung potentieller Bedrohungen ist dieses Team mit der Bearbeitung von Sicherheitsvorfällen betraut. Dies umfasst sowohl die Incident Response (IR) und die Vulnerability Response (VR) als auch das Abuse-Handling.

Dieses Team muss organisatorisch mit den entsprechenden Befugnissen ausgestattet werden, um in Notfällen Maßnahmen ergreifen zu können, die den Betrieb des betroffenen Systems ggf. einschränkt, um die Sicherheit der nicht betroffenen Systeme zu gewährleisten.

4 Strukturierung von Meldungen

Die im Folgenden vorgeschlagene Struktur orientiert sich an dem Common Announcement Interchange Format (CAIF¹) vom RUS-CERT.

- Identifikation des Dokumentes:
 - o Issuer (Herausgebende Organisation)
 - o Announcement ID (z.B. eine fortlaufende Nummer)
 - o Typ des Dokumentes ("type")
 - o Dringlichkeit ("urgency": Alert, Warning, Advisory, Informational)
 - o Stufe ("level": brief, full, digest, other)
 - o Geschmack ("flavor": vulnerability-description, patch-notification, heads-up, other)
 - o Restriktionen über die Weitergabe des Dokumentes ("interchange restriction": constituency, none)
 - o früheste Veröffentlichung- sofern das Dokument z.B. schon zwischen den kooperierenden Stellen verteilt werden aber erst zu einem späteren Zeitpunkt in die Öffentlichkeit gelangen soll.

¹ <http://cert.uni-stuttgart.de/projects/caif/>

- Zielgruppen, für wen ist das Dokument verfasst, bzw. für welche Zielgruppen von Lesern sind Inhalte im Dokument vorhanden ("target-groups": lang, tech-background, orga-overview, environment), (optional)
- Constituencies - Beschreibung der Klientel, für die Information enthalten sein kann. Im Text selbst kann auf diese Beschreibung referenziert werden. Z.B. können Abschnitte eingefügt werden, die sich speziell auf eine konkrete IT-Infrastruktur einer Einrichtung beziehen. Solche Abschnitte können vor einem Austausch des Dokumentes an andere Einrichtungen automatisch entfernt werden. (optional)
- Revisionen, Geschichte des Dokumentes mit den Daten von Änderungen und Neuveröffentlichungen des Dokumentes. ("revisions")
- Kategorisierung der Plattform, des Produktes und des Protokolls auf das sich das Dokument bezieht. Dies kann auch eine frei gewählte Kategorie sein. Es bietet sich an, einen Katalog von möglichst generischen Kategorien zentral zu pflegen. ("category")
- Titel des Dokumentes ("subject")
- Zusammenfassung des Inhaltes ("summary")
- Problemaspekte
 - o Problem ID zur Identifizierung eines Problems, wird z.B. von CVE oder iCAT vergeben. ("id") (optional)
 - o Klasse ("class": buffer-overflow-bug, format-string-bug, insecure-configuration, insecure-defaults, design-flaw, programming-flaw, malware, other) (optional)
 - o Angriffs-Vektor- Einfallstor für einen erfolgreichen Angriff. Diese Information kann helfen, temporäre Gegenmaßnahmen, wie z.B. Firewallkonfigurationen, zu ergreifen. ("attack-vector") (optional)
 - o Angriffs-Voraussetzungen- welche Ressourcen sind für einen Angriff erforderlich? ("attack-requirements") (optional)
 - o Angriffs-Signatur- welche Spuren hinterlassen Angriffe auf dieses Problem? ("attack-signature") (optional)
 - o Auswirkung- welche Auswirkung hat ein erfolgreicher Angriff im schlimmsten Fall? ("impact") (optional)
 - o technisches Risiko- Einschätzung des Risiko in einem Worst-Case-Szenario ("risk") (optional)
 - o Eintrittswahrscheinlichkeit bezogen auf eine spezielle Constituency (s.o.) ("probability-of-occurrence") (optional)
 - o Bedrohung- Einschätzung der Bedrohung für eine spezielle Constituency (s.o.) ("threat") (optional)
 - o Exploit Status- Information über die aktive Ausnutzung des Problems und die Verfügbarkeit automatisierter Angriffsprogramme ("exploit-status") (optional)
- Mildernde Faktoren- können z.B. sein, dass ein betroffener Dienst nicht voreingestellt aktiv ist. ("mitigation") (optional)
- Betroffene Systeme- eine Liste der von dem beschriebenen Thema oder Problem betroffenen Systeme ("affected", optional)
- Nicht betroffene Systeme- sofern bekannt ist, welche Systeme von dem Problem betroffen sind ("not-affected") (optional)
- Möglicherweise betroffene Systeme- Liste von Systemen von denen nicht bekannt ist, ob sie betroffen sind, es aber auch nicht ausgeschlossen werden kann. ("possibly-affected") (optional)
- Feststellen der Verwundbarkeit- Anleitung oder Skript oder Programm in beliebigen Formaten, die einen Anwender in die Lage versetzen, festzustellen, ob eine Infrastruktur betroffen ist oder nicht. Hier können fremde Formate, wie z.B. OVAL oder AVDL integriert werden. ("determine-affectedness") (optional)
- Kontext- Technische Beschreibung des betroffenen Systems und Verwendungszweck. Dies kann unerfahrenen Administratoren helfen, zu identifizieren, ob sie das System benötigen oder nicht. ("context") (optional)
- Beschreibung des Problems. Detaillierte Beschreibung des Problems. ("description") (optional)
- Workaround- temporäre Maßnahmen um das Problem zu mildern oder zu beseitigen, ggf. unter Betriebseinschränkungen ("workaround") (optional)
- Gegenmaßnahmen- Maßnahmen, die das Problem endgültig beseitigen, z.B. ein Patch. ("solution") (optional)
- Weitere beliebige Sektionen ("arbitrary") (mehrfach optional)
- Referenzen zu Quellen und weiterführenden Dokumenten ("bibliography") (optional)
- Credits (optional)
- Disclaimer (optional)