Bearbeiten von Sicherheitsvorfaellen

[Die Benachrichtigung] [Was macht der Security-Kontakt?] [Wie erfährt das CERT von den Problemen?] [Weitere Unterstützung] [Bitte um Rückmeldungen] [Das Kleingedruckte]

Bearbeiten von Sicherheitsvorfällen

Die Benachrichtigung

Wenn das ACOnet-CERT einen IT-Sicherheitsvorfall im ACOnet erkennt oder darüber informiert wird, sendet es eine **E-Mail**-Nachricht an den **Security-Kontakt** des jeweiligen ACOnet-Teilnehmers (z.B. Universität, Fachhochschule, Studentenheimträger, Museum, etc...). Darin steht:

- **wo** der Vorfall passiert ist (die IP-Adresse, Webseite, ...),
- **worin** das Problem besteht (Virus-Infektion, Spamversand, DoS-Angriffe, ...),
- anhand welcher **Hinweise** (Logfiles, Blacklisteneinträge, ...) das CERT das Problem erkannt hat,
- soweit möglich und sinnvoll auch **Hintergrundinformationen, Erläuterungen, Empfehlungen,**
- eine Bitte um **Rückmeldung**,
- eine elektronische **Unterschrift**.

Was macht der Security-Kontakt?

Jede Organisation im ACOnet organisiert ihre Prozesse zur Behandlung von Sicherheitsvorfällen entsprechend ihren Möglichkeiten und Bedürfnissen selbst. Im Wesentlichen geht es darum, die zuständigen Personen (z.B. Systemadministratoren) zu ermitteln und zu veranlassen, daß das Problem behoben wird.

In den meisten Fällen ist ein Computer mit Schadsoftware infiziert worden. Oft reicht ein (aktualisierter) Virenscanner aus, um die Schädlinge loszuwerden, mitunter wird eine Boot-CD benötigt, um den Scan von einem sicheren Betriebssystem aus durchzuführen. Übrigens heißt ein Malwarebefall keineswegs, daß der Computer schlecht gewartet wäre oder daß damit zweifelhafte Webseiten aufgerufen worden wären!

Seltener sind die Fälle, wo in einen Server eingebrochen wurde und z.B. Phishing-Seiten auf einen Server gelangt sind. Dies ist stets eine Herausforderung für die/den Systemadministrator/in/n/en, denn es muß:

- zunächst das offensichtiche Symptom (Phishing-Seite, ...) behoben werden,
- die Sicherheitslücke identifiziert und geschlossen werden,
- genau untersucht werden, welche Manipulationen außerdem am Server vorgenommen wurden (z.B. Entwenden von Paßwörtern, Infektion von Dateien, Installation von Backdoors, Rootkits...),
- hilfreich wäre es, gegebenenfalls im Zuge der Untersuchung weitere betroffene Systeme (z.B. Angreifer) zu identifizieren.

Wie erfährt das CERT von den Problemen?

Die Informationsquellen des CERT umfassen neben Daten aus dem ACOnet-eigenen Betriebsbereich (z.B. Netzwerstatistiken, diverse Sensoren) auch Informationen von Dritten (z.B. einschlägige Websites, Blacklisten, etc...) und natürlich auch Meldungen und Beschwerden, die individuell an das CERT herangetragen werden.

Das CERT prüft und bewertet diese Informationen im Rahmen seiner Möglichkeiten und Erfahrungen mit höchstmöglicher Sorgfalt, aber Irrtümer und Fehldiagnosen sind unvermeidlich. Dabei ist immer abzuwägen:

- das Risiko, vor einem Problem zu warnen, das es nicht gibt, gegen
- das Risiko, vor einem tatsächlichen Problem vorsichtshalber nicht gewarnt zu haben.

Das CERT ist bemüht, möglichst transparent die ihm vorliegenden Informationen auch an die ACOnet-Teilnehmer weiterzugeben. In diesem Sinn werden die häufigsten Hinweise in den E-Mail-Benachrichtigungen des CERT mit einem **Tag** versehen, anhand dessen weitere Informationen dazu auf der Seite Incident Handling - Tags abgerufen werden können.

Weitere Unterstützung

Das ACOnet-CERT-Team unterstützt die Security-Kontaktpersonen der ACOnet-Teilnehmer bei Bedarf:

- durch seine Kontakte zu Herstellern und Firmen
- mit Informationen, die CERT-Kreisen vorbehalten sind
- durch die gesammelten Erfahrungen aus dem ACOnet
- indem es den Kontakt mit einschlägigen Experten in der Community herstellt.

Es versteht sich von selbst, daß das CERT dabei stets die nötige Diskretion walten läßt und auf allfällige Geheimhaltungsvereinbarungen Bedacht nimmt.

Das ACOnet-CERT-Team kann leider keine Unterstützung für Endanwender anbieten. Schon aus personellen Gründen ist das nicht denkbar, wäre aber auch nicht sinnvoll, da das CERT nicht über die lokalen Gegebenheiten bescheid weiß, wie z.B. Campus-Lizenzen, Organisation des Netzwerks, Zuständigkeiten, Services, Logfiles...

Anwender wenden sich bitte an ihre Netzwerkadministratoren oder den Helpdesk der eigenen Institution.

Bitte um Rückmeldungen

Das CERT **ersucht um Rückmeldungen**, wenn und wie ein Fall gelöst wurde:

- für die oben erwähnte Bewertung der Problemhinweise ist die Erfahrung "im Feld" nötig
- das macht es möglich, frühzeitig zu warnen, sollte die Problembehebung fehlgeschlagen sein
- zu wissen, welche Malware oder Hackmethoden häufig auftreten, macht es dem CERT möglich, gezielt nach weiteren eventuell ebenso betroffenen Rechnern zu suchen
- können beteiligte Rechner – als Angreifer oder als Opfer – identifiziert werden, verständigt das CERT auf geeignete Weise die jeweils in Frage kommenden CERTs, Netzbetreiber, etc.
- gesammelte Erfahrungen fließen in die Behandlung weiterer Fälle ein

Routinemäßig beobachtet das CERT auch vorerst abgeschlossene Fälle noch mindestens eine weitere Woche. Das hat einerseits den Zweck, spät eintreffende Hinweise noch richtig zuordnen zu können, und andererseits sicherzugehen, daß das Problem tatsächlich gelöst werden konnte.

Das Kleingedruckte

Hinweise und Empfehlungen des CERT müssen von den ACOnet-Teilnehmern selbst auf ihre Richtigkeit und Anwendbarkeit geprüft werden! Da die Tätigkeit des CERT regelmäßig darin besteht, vage, unvollständige, mehrdeutige Informationen, häufig von Dritten, zu deuten, muß es zwangsläufig manchmal zu Fehlinterpretationen kommen. Das ACOnet bzw. ACOnet-CERT kann daher keine Haftung für im Rahmen des CERT-Service getroffene Aussagen übernehmen.

Das CERT empfiehlt ganz besonders, die Gültigkeit der elektronischen GPG-Signatur zu prüfen, um die Authentizität unserer Hinweise sicherzustellen.