Datensicherheit in Zeiten von Würmern, Viren und Nutzerfehlern

IKS GmbH Jena
Information – Kommunikation - Systeme
Leutragraben 1
D-07743 Jena

Telefon: +49-3641-460850
Fax: +49-3641-460855
eMail: L.Donnerhacke@iks-jena.de
Internet: http://www.iks-jena.de

Zur Firma

- **Gründung im Januar 1996**
- **Beratung, Konzeption, Realisierung und Betrieb komplexer Informations- und Kommunikationssysteme**
- **redundantes IP Netz mit autonomen System**
- **Outsourcing kompletter EDV Dienstleistungen**
- **Sicherheitsbetreuung, Firewall- und VPN Verbindungen**

KS GmbH
Information
Kommunikation
Systeme

Was ist sicher?

- **Sicherheit liegt im Auge des Angreifers**
- **Ein System ist sicher, wenn der Angreifer mehr investiert als er herausbekommt (Betrachtung im konkreten Fall)**
- **Erst in der Summe über alle möglichen Fälle ergibt sich eine Gesamtsicherheit**
- **100% sichere Systeme sind stets weiter angreifbar**
- **Restrisiko durch Versicherungen abfedern**
- **Sicherheit ist ein Prozeß, kein Zustand**
  Deshalb: Permanente Überprüfung notwendig

KS GmbH
Information
Kommunikation
Systeme

Typische Angriffe

- **80% aller Angriffe kommen von innen**
- **Über 95% aller erfolgreichen Angriffe kommen von innen**
  D.h.: Die meisten Angriffe waren befugt!
- **Ausspionieren von Daten**
- **Veränderung von Daten**
- **Unterschieben von fremden (Schad)Programmen**
- **Vorspieglung falscher Kommunikationspartner**
  (Phishing, Terminvereinbarungen, Rechnungen, ...)
- **Agieren für Dritte: Spamming, Basis weiterer Angriffe,**
  Hosting von Pornoseiten, ...
- **Überlastung durch Massennutzung: DoS**
- **Überlastung der Infrastruktur: DDoS**

Einfallstore

- Installation durch den Nutzer selbst
- Ausnutzen von Programmfehlern zur Start von Code
- Ausnutzen von Programmfehlern zur Fernsteuerung
- Laxheit der Nutzer im Umgang mit Passworten
- Schwache Passworte

Viren, Würmer und Trojaner

- **Virus: Selbstverbreitender Code auf dem Wirtssystem**
- **Wurm: Selbstverbreitender Code zwischen Wirtssystemen**
- **Trojanisches Pferd: Code, der im Hintergrund bösartig ist**
- **Infektion neuer Systeme durch Viren nur durch den Anwender selbst möglich**
- **Infektion neuer Systeme durch Würmer durch Programmfehler**
- **Trojaner werden vom Anwender selbst installiert**

KS GmbH
Information
Kommunikation
Systeme

Verteidigungsvarianten

- **Software aktuell halten**
- **Systeme so einstellen, daß Nutzer nichts installieren können**
- **Nutzer aufklären**
- **Unsichere Authenisierungen, wie Passworte, durch Smartcards ersetzen**
- **Verschlüsselung schützt vor Einblicken (VPN, PGP, S/MIME)**
- **Signaturen schützen vor Veränderung (PGP, S/MIME, DNSSEC)**
- **Schlüsselinfrastruktur (PKI) schützt vor Identitätsklau**
- **Virenscanner? Nutzt bei veralteter Software. Besser Updaten!**
- **Zero-Day-Exploit: Ausnutzen neuer Schwachstellen, kein Schutz durch Virenscanner oder Update möglich**
- **Kommunikation mit Firewalls beschränken**

DoS, DDoS und Spam

- Trennung in „erwünscht“ und „unerwünscht“
- Bei Mail: Klassifizierung durch Spamfilter
- Firewalls als Filter gegen externe DoS Angriffe
- Ratelimits meist in Anwendungen praktikabel
- Dienste nur anbieten, wo zwingend notwendig
- Eigene Systeme bei DDoS nicht betroffen
- Dezentralisierung der Angebote zum Schutz vor DDoS
- DDoS Schutz nur durch externe Hilfe möglich

Beispiel DNSSEC

;; ANSWER SECTION:
www.edri.org. 13598 IN **A** 213.84.134.66
www.edri.org. 13598 IN **RRSIG A** 5 3 57600 20060411224816 (
20060312224816 5579 **edri.org.**
H0op/k4NA3xkcw5NsY3raPPm5C898bYwIi++hyai7GJj
98B0MkhUA7ct0KrUd6JprnMwRC3fjqd/yTN2DZAO8xqc
fLYJIThnf09AFrhhI+DHeeTqWPYIFey7bXTXFNY8UcXN
3GIoKJuABSs1Kc4p/wO2EK4cH8JHtwd1A1lQS1Y=)

;; AUTHORITY SECTION:
edri.org. 13598 IN **NS** avalon.iks-jena.de.
edri.org. 13598 IN **NS** euro-ns1.cw.net.
edri.org. 13598 IN **NS** euro-ns2.cw.net.
edri.org. 13598 IN **NS** euro-ns3.cw.net.
edri.org. 16124 IN **RRSIG NS** 5 2 57600 20060411224816 (
20060312224816 5579 **edri.org.**
cY7TPEJtvo2Mhf8e9gH7lqb8ZUusUGDuO3paZSoKHsIZ
fp3dGt7n/R3Se0vOevG3Aqk7tjIVCGiJvdJubvaLENy4
YRDBnalViWJBU5k9We9JvF3jUO5boGAVOANL29T1zy1b
nu6ggt8aMSnhfEwe6VPEaMOgg8XhxN/Vtzn/7iU=)

Beispiel DNSSEC (PKI)

;; ANSWER SECTION:

edri.org. 57600 IN **DNSKEY** 256 3 5 (
AQOtC1r11si4GFtHOO8LSnR42vY0l0g2OEl2IAcu0Q0J
itA7ArB5h3cy5vzic6fslE6SyrzQdS6v7Sba6QmZIpec
iXyCKcLbDbxOh0v/rwnp1Vb31wijF06jJgECXzznU5OZ
v3Cdd/cJI4aNeJIVY1VOI/cdwYGGpdVrVOPWMJE48w==
) ; key id = 5579

edri.org. 57600 IN **DNSKEY** 257 3 5 (
AQPeBHBe2Q10MGKWy+qxUOz6kFL8/XhWXb7jbuxgH85P
QHALxZg7bfHaeKsJRGEXIvD2/aMPotEYHHb5o3/qfn9u
MzaYb5LUKNUAUSJbRkpQltFMmJoGPhtZHRUzcxp7nfaN
anZ9r6b7aoGoj1zVKuq38XPtvgQ9rmU4/3Fk4xGWducw
RudCqaNHBC9L2wDKaW5Jel7hGlgRMV5gCLgcxydiv3Vm
V5WiSwS3uMuDf1iR3vp+wvGthrevTGrsEHRP6PwUJP6e
erbgoFK14JWKbyvx9BHkeDBlZ+k2RxcRgOffDsak7GCp
GL8biiqZ3F624mCrDujBTvs6RwQbctQ8c9wp
) ; key id = 41127

Ohne RRSIG Records

Beispiel DNSSEC (PKI)

;; ANSWER SECTION:
edri.org.dnssec.iks-jena.de. 57600 IN **DLV** 41127 5 1 (
A6330904D067A7CC29B6E6B6754DC3043B952F95)
edri.org.dnssec.iks-jena.de. 57600 IN **RRSIG DLV** 5 5 57600 20060416223108 (
20060317223108 890 **dnssec.iks-jena.de.**
cSXH0fw5eWwtNnmpVk9a6WLVoPQkj12mq28sbcfbDw4O
mhTA40TFTMPjH2KH6F8lAUpt9/8g+L9fqm8Df+3nsGTe
F91I4Fv0SVd2K0tZh/9nc8bsahPxJY929+w8vYfjxSR/
WizvsQsUC4VHK+mkOW3dakwy7PlAsZQ3SGLbJbg=)

;; ANSWER SECTION:
8.d.b.4.1.0.0.2.ip6.arpa. 172800 IN **DS** 39105 5 1 (
E51755C43A0FF7149B07CD2C6C22DF291D91CE30)
8.d.b.4.1.0.0.2.ip6.arpa. 172800 IN **RRSIG DS** 5 10 172800 20060420100504 (
20060321100504 50126 **b.4.1.0.0.2.ip6.arpa.**
e0RZZa0dmZ1OX1VjxahyOCluvcYhQuFOWLWYrJ6aCuhg
4ag4uBRPkzfITG8zez5aaVH6sy1it/4rhDEaeikIgEiR
Dr27/Zgxv1b7x1BJUutUCY+egKM5nPa9t1DyLdDxT2qY
D76YqHAZNdhr2kxwnTQmLctdFoe1lM1BxxtDkrlGx+Gx
uZ4AXdw+hxQQCwxVRG0ct66F)

Fragen?

OpenPGP

pub 1127R/DB089309 1997-03-17

Lutz Donnerhacke <lutz@iks-jena.de>

Key fingerprint 1C 1C 63 11 EF 09 D8 19
E0 29 65 BE BF B6 C9 CB