Informationssäkerhet
För utvecklare

Roland Ronquist

NORDLO

Planering

16/8 Tisdag – Introduktion, översikt, reflektion

17/8 Onsdag – Kryptoteknik, PKI; certifikat, signaturer, nyckelutbyte….

23/8 Tisdag – Programmering, fallgropar, fel och problem

24/8 Onsdag – Åtgärder, penetrationstest, revision, intrångsdetektering, skalskydd

30/8 Tisdag – Administrativa åtgärder, regler, myndigheter, avrundning

31/8 Onsdag –

Översikt

Vad är säkerhet och vad kan vi göra?

- Dataintegritet
- Åtkomstkontroll
- Spårbarhet
- Personlig integritet

Översikt

Personlig integritet

- Epost
- Webb
- Sociala nätverk
- Annonser

Vanliga hot

- Nätverksinfrastruktur, protokoll, utrustning
- Buffer overflow, cross site scripting, ”intressanta” funktioner i webbläsare och javascript
- Internet of things, telefoner m.m.
- Social engineering
- Biblioteksfunktioner, stödsystem (databaser, sql-injection)
- Drive by, ransomware,

Översikt

Vad är säkerhet och vad kan vi göra?

- Identifiera kritiska system och kritisk information
- Säkerhetskopiering och redundans
- Tvåfaktorsautenticering, PKI, VPN...
- Spårbarhet, loggar, övervakning
- Kryptonyckel kontra krypteringslösenord
- Verifierad uppstart

Översikt

Social engineering, drive by, ransomware, sqlinjection, buffer overflow, PKI, kodrevision, cross site scripting, bounds checking, pekare, användarinput, privilegium, eskalering, integritet, autenticering, metadata, tracking cookie, cookie, röjande strålning, nyckelutbyte, assymetrisk kryptering, RSA, sidokanaler, cpu-buggar, blockkedja, smart card

Översikt

Bra lösenord…

82#&yAzzP1-ruPm

Hej tomtegubbar slå i glasen och leva mycket rövare och tok

Översikt

Social engineering är ett bekant begrepp

Motiverade och lojala medarbetare är en ofta glömd faktor.

Kritisk information och kritiska system

- Vad gör vi utan IT-stöd? Hur då? Nödåtgärder?
- Vilka system behövs verkligen i den dagliga driften? Rangordna, motivera, diskutera!
- Vilka risker förknippas med våra prioriterade system?
- Hur återställer vi?

Säkerhetskopiering - backup

- Ofta bandbackup i seriösa sammanhang fastän disk är billigare
- Bandrobotar som själv byter band
- Backup till disk billigt
- Backup över nät smidigt

Säkerhetskopiering - återställning

- Systembackup ”bare metal” kan vara praktisk men leder ofta till problem när den nya maskinen inte är identisk med den gamla
- Filbackup, återställningen måste vänta tills operativsystemet är installerat på den nya maskinen, ibland krävs fler program än så

Säkerhetskopiering - backupschema

Det är dyrt att lagra information, därför använder man ofta ett schema för hur länge olika filer sparas, ett exempel skulle kunna vara att man gör såhär:

- Måndag – lördag sparas de kopierade filerna en vecka
- Söndag sparas kopian en månad
- Sista söndagen i månaden sparas kopian i 12 månader
- Sista dagen på året sparas kopian i 10 år

Lagringssystem - RAID

Redundant Array of Independent Disks

informationen sprids över flera diskar så att detta åstadkoms:

- Större lagringsutrymme
- Snabbare dataåtkomst
- Säkrare lagring

men bara två av dessa punkter på en gång

Lagringssystem - RAID

RAID är inte backup

- Ransomware förstör ändå
- Många diskfel märks inte förrän efter omstart
- Fysiska fel, översvämning, brand och åska drabbar alla diskarna

Verksamhetskritiska system

- Vad är ett verksamhetskritiskt system?
- Hur skyddar vi dem?
- Hur återhämtar vi oss efter ett haveri?
- Säkerhetskopiering?
- Redundanta system?
- Reservkraft; brand och andra naturkatastrofer

Skalskydd

- Brandvägg
- Tvåvägsautenticering
- PKI
- VPN
- Brandvägg
- Nätverkspartitionering

Haveriåterhämtning

- Rutiner
- Nödsystem
- Bare metal recovery
- Beredskapsplanering
- Beredskapsövningar

Datalagring

- Säkerhetskopiering
- RAID
- Molnlagring
- Multipla lagringscenter

Fungerar säkerhetskopieringen?

¡ Säkerhetskopieringssystemet måste verifieras !

- Hur hanterar vi databaser och liknande saker?
- Epost och andra kommunikationssystem?
- Bare metal kontra högre nivå
- Hur lagrar vi våra säkerhetskopior? Varför?
- Juridiska krav och begränsningar?

Fungerar säkerhetskopieringen?

- Databaser, epost, kommunikationssystem m.fl. kräver ofta specialåtgärder vid backup för att informationen skall vara logiskt sammanhängande och korrekt
- Bare metal betyder att all information i datorn säkerhetskopieras så att systemet kan återställas på en ny dator utan att någon behöver installera OS först. Det finns inte några garantier att operativsystem, drivrutiner fungerar på en ny maskin om den inte är 100% kompatibel
- Ekonomisk bokföring lagras 10 år, det finns andra sorters information (ofta rörande miljö, hälsa och säkerhet) där informationen måste lagras längre tid enligt lagen.

Lagringssystem

RAID är inte säkerhetskopiering!

Var finns våra data? Hot? Möjligheter?

Hur kommer vi åt informationen?

Kryptering, åtkomstkontroll, integritetskontroll

Kryptoteknik

- Certifikat
- Signaturer
- Hashar
- Symetriska chiffersystem
- Assymetriska system

Hash-funktioner

En hashfunktion används för att göra ett ”fingeravtryck” på en fil eller en datapost med någon form av statistisk konfidens.

En hasfunktion liknar de checksummor som används inom exempelvis telekommunikation, men de funktioner man använder där är oftast inte optimerade för hög statistisk säkerhet.

Exempel: md5, sha1, sha128, sha256...

Symetriska krypteringssystem

Med ett symetriskt chiffersystem används **samma** kryptonyckel för att kryptera som för att dekryptera informationen.

Detta är ofta det lekmän tänker på när de talar om kryptering.

Det finns en rad välkända algoritmer, Enigma, RC4, Blowfish, DES, AES….

Assymetriska chiffersystem

Två olika kryptonycklar, en för att kryptera och en annan nyckel för att dekryptera, hämta tillbaka klartexten.

Ofta långsamma och de kräver långa nycklar.

RSA, Eliptic Curves

Digitala signaturer

Att signera en fil eller ett meddelande kräver flera steg:

- Först hashar vi den med en känd hashfunktion
- Sedan krypterar vi hashen med vår hemliga nyckel vilket ger oss signaturen
- När någon vill verifiera signaturen så beräknar hen först hashen och sedan dekrypterar man signaturen med vår publika nyckel
- Är då båda hasharna lika så är filen med hög sannolikhet intakt

Digitala certifikat

Ett digitalt certifikat är en strukturerad datafil med en digital signatur. Filen innehåller information både om filens ägare och om utställaren för certifikatet (CA), men filen kan innehålla fler saker vid behov. Framför allt brukar de innehålla kryptonycklar för att innehavaren skall kunna använda assymetrisk kryptering.

Med hjälp av utställarens publika nyckel kan sedan certifikatets äkthet verifieras.
Den dominerande certifikatstandarden är X.509

PKI Public Key Infrastructure

- Nyckelkedjorna är hierarkiska med root-CA:ns nyckel i toppen.
- Det finns många utställare vilket krånglar till administrationen
- Nyckelrevokering är ett annat problem som ofta ignoreras
- De flesta PKI-tillämpningar fungerar med egentillverkade nycklar