

PaxLog

Kunde: Mads Skjern A/S
Konsulent: Nis Peder Bonde, SecuriPax
Dato: 24-03-2008
Periode: Januar - Februar 2008

Konklusion

Jeg har d.d. gennemgået logmaterialet fra Mads Skjernes sikkerhedssystemer vedrørende ovennævnte periode. Der har i perioden været enkelte sikkerhedsmæssige hændelser, som jeg beskriver nedenfor i større detaljer med forslag til korrigerende handlinger.

Kommentarer af sikkerhedsmæssig karakter

Trojansk hest

Pc'erne xxx, xxx, xxx, xxx, og xxx er inficeret med en trojansk hest, som forsøger at kommunikere med sin Command & Control Botnet server via IRC trafik.

Den trojanske hest vil muliggøre, at uvedkommende kan kontrollere pc'erne og derfra opnå adgang til følsomme systemer på virksomhedens netværk.

Da det kan være særdeles vanskeligt at fjerne trojanske heste vil jeg anbefale, at man i stedet reinstallerer pc'erne fra bunden. Samtidig kan man med fordel udspørge brugerne for at finde ud af, hvordan pc'erne kan være blevet hacket.

Værktøjer til fjernstyring

Der har også i denne periode været en del trafik fra programmer til fjernstyring af pc'er. Jeg har således kunnet konstatere, at en del af virksomhedens brugere hyppigt gør brug af sådanne værktøjer, hvorved personer uden for virksomheden opnår mulighed for at fjernstyre virksomhedens pc'er.

En del af disse forbindelser etableres v.h.a. produkter, som også kan give mulighed for, at medarbejderne selv kan overtage deres pc'er på virksomhedens interne netværk, når de er på rejser m.m. Altså hvor medarbejderne installerer programmer på deres pc'er, som muliggør en form for selvetablerede VPN forbindelser uden for it-afdelingens kontrol og uden den sikkerhed, som virksomheden ellers kræver ved fjernadgang.

I perioden har jeg f.eks. kunnet konstatere følgende:

- VPN-brugeren NN har i stort omfang gjort brug af programmet LogMeIn, som sandsynligvis anvendes til, at brugeren selv kan overtage kontrollen med sin pc fra en hvilken som helst pc på Internettet.
- En række brugere har anvendt GotoAssist eller GotoMyPc. Jeg kan i loggen ikke skelne om der er tale om den ene eller den anden slags program.

Jeg frygter, at dette kan give uvedkommende adgang til virksomhedens interne netværk og systemer med alvorlige konsekvenser til følge. Jeg vil derfor anbefale, at it-sikkerhedsudvalget overordnet tager stilling til, om man vil acceptere, at medarbejderne anvender sådanne værktøjer – og i givet fald under hvilke retningslinjer. Altså at udvalget fastlægger en politik for anvendelse af sådanne programmer til fjernstyring.

Til Begrænset Fordeling

Skype

Også denne gang har forskellige brugere på Mads Skjerns systemer gjort flittig brug af Skype. De primære brugere lader til at være:

- Pc'en med ip-adressen 192.168.30.130 i Langt-bort-istan
- Pc'en XXX
- Pc'en "ALEXACER" med MAC-adressen 00:16:D4:Bo:49:A4 på netværket i Korsbæk (på datoerne 10/1, 14/1 og 19/1). Der er muligvis tale om en besøgende konsulent.
- Brugeren XXX
- Brugeren XXX

Skype er et problematisk system, som hyppigt er blevet misbrugt til spredning af virus og orme. Jeg vil anbefale, at ledelsen klart melder ud til alle brugere, at den slags programmer ikke er tilladt i koncernen.

Fremmede pc'er på nettet

Jeg har kunnet konstatere, at der denne gang har været fremmede pc'er på virksomhedens interne netværk fra følgende virksomheder: <en længere liste af danske og udenlandske virksomheder>

Det er potentielt meget farligt at lade fremmede pc'er komme på Mads Skjerns netværk, da de vil kunne sprede virus og orme til virksomhedens pc'er og servere.

Det nye gæsternetværk forventes at fjerne behovet for, at sådanne brugere tilkobler deres pc til Mads Skjerns interne netværk, og jeg vil anbefale, at der på tværs af de forskellige afdelinger laves en klar politik for gæstepc'ers netværksadgang.

PaxScan resultater

På baggrund af den kontinuerlige scanning af Mads Skjerns offentligt tilgængelige IP-adresser og services, kan jeg konkludere, at der i perioden generelt kun har været mulighed for fra Internettet at etablere forbindelser til de af virksomhedens systemer, som det er hensigten, at der skal være ekstern adgang til.

Det er således min opfattelse, at virksomhedens firewall-systemer er konfigureret korrekt og yder de bagvedliggende systemer den tiltænkte grad af beskyttelse.

Den gennemførte applikationsspecifikke scanning viser, at der p.t. ikke har kunnet findes nogen alvorlige sårbarheder i de scannede systemer, men har dog afsløret enkelte uhensigtsmæssigheder:

1. Scannings-softwaren har vist, at WWW-serveren er sårbar overfor en "low" risiko relateret til den såkaldte "ReadDesign" sårbarhed. På følgende adresse kan man læse mere om sagen og ligeledes få anvisninger til at udbedre problemet: <https://www.appsecinc.com/Policy/PolicyCheck1520.html>.
2. CSG serveren har NTLM autentifikation aktiveret. Dette bør deaktiveres, da der ikke er behov herfor. Risikoen er lille.
3. Nianets routere i Korsbæk har en åben port, som tillader at kommunikere med en NTP dæmon på routerne. Dette er ikke nødvendigt, hvorfor jeg vil anbefale, at Nianet kontaktes med en anmodning om at lukke for denne funktionalitet. Hvis der på et tidspunkt skulle blive konstateret en sårbarhed i NTP dæmonen vil den nuværende åbning kunne give basis for et Denial Of Service angreb mod Mads Skjerns Internetforbindelse, så ikke-anvendte services som denne bør deaktiveres.
4. Der er ikke rapporteret om identificerede sårbarheder i relation til E-handel systemet.

Til Begrænset Fordeling

Kommentarer af driftsmæssig karakter

Til Begrænset Fordeling

PaxScan

Generelt

Den udarbejdede PaxScan rapport viser et øjebliksbillede af resultaterne af den portscanning, som kontinuerligt udføres mod Mads Skjerns offentligt tilgængelige IP-adresser fra SecuriPax's systemer. Formålet med portscanningen er at identificere, hvilke af virksomhedens systemer og services, som kan tilgås via Internettet, og som en hacker dermed måtte være i stand til at forsøge at angribe udefra.

Derudover er der også udarbejdet en rapport, som på baggrund af en applikationsspecifik scanning giver et øjebliksbillede af sikkerheden i de systemer, som der tillades offentlig adgang til.

Omfang

For hver af de offentligt tilgængelige IP-adresser (alle afdelinger men ingen hjemmearbejdspladser), er der gennemført følgende scanninger:

1. En såkaldt ping-test, som viser om systemet svarer på "ping" pakker.
2. En såkaldt TCP Syn scanning af samtlige 65.535 mulige TCP portnumre.

Der er derimod ikke foretaget nogen scanning af de såkaldte UDP porte, da tilstedeværelsen af firewall's i systemet medfører, at man ikke umiddelbart er i stand til at afgøre, om en given UDP port er beskyttet eller er åben for ekstern adgang.

Denne vanskelighed skyldes rent tekniske forhold i specifikationen af UDP protokollen, som er af en helt anden karakter end TCP protokollen. Det positive er dog, at evt. hackere også vil være hæmmet af de samme tekniske forhold og dermed heller ikke nemt vil kunne finde ud af, hvilke porte der måtte være tilgængelige udefra.

Det er min hensigt på et senere tidspunkt at udvide PaxScan til også at omfatte en kontrol af de vigtigste og mest sårbare UDP porte. Dette vil dog kræve anvendelse af andre scannerværktøjer, som jeg endnu ikke har integreret i systemet.

Herudover er der gennemført en applikationsspecifik scanning mod de systemer, som er blevet identificeret som værende offentligt tilgængelige ved den forudgående portscanning.

Værktøjer

Ved scanningen har jeg anvendt et specialudviklet program til at styre den overordnede scannings-proces, sikre at alle kontroller gennemføres korrekt, indsamle resultaterne og præsentere de væsentligste elementer heraf i en overskuelig form, som muliggør kommentering af resultatet.

Selve scanningen er udført ved anvendelse af de offentligt tilgængelige programmer som *NMAP* og *Nessus*.

Synergi mellem scanning og loganalyse

En portscanning er baseret på en analyse af den netværkstrafik, som kommer tilbage fra det scannede system, når man forsøger at tilgå de forskellige porte. Det betyder imidlertid, at scanningen i sig selv ikke kan vise, om der skulle slippe pakker igennem det første sikkerhedslag (ydre firewall), som efterfølgende måtte blive afvist af det andet sikkerhedslag (indre firewall).

Dette vil derimod afsløres ved PaxLog analysen af den indre firewall's loginformationer, hvorved man som en synergieffekt af PaxScan og PaxLog opnår fuld vished for, at sikkerheden i den ydre firewall er intakt og virksom.

Til Begrænset Fordeling

Begrænsning

En portscanning er således først og fremmest en test af, om virksomhedens firewall-systemer er konfigureret korrekt og yder alle interne netværk, systemer og services den beskyttelse mod ekstern adgang, som er hensigten. Derimod kan en portscanning ikke vise, om de eksternt tilgængelige systemer rent faktisk skulle være sårbare overfor eventuelle hackerangreb.

Dette er derimod delvist omfattet af den supplerende applikationsscanning, som ved anvendelse af et dertil egnet værktøj kan afgøre, om systemerne skulle være sårbare overfor de hackerangreb og hackerteknikker, som er kendt på nuværende tidspunkt, og som er af en sådan karakter, at man overhovedet er i stand til at foretage en automatisk test heraf.

Det skal dog understreges, at den gennemførte applikationsscanning er en basal scanning mod de mest udbredte sårbarheder, som typisk først vil blive forsøgt anvendt af hackere. Scanningen er først og fremmest rettet mod den systemsoftware, som benyttes på de pågældende maskiner, mens f.eks. web-applikationer o.l. ikke er omfattet heraf.

Logmaterialet

Der er i perioden blevet opsamlet og behandlet logmateriale fra følgende sikkerhedssystemer:

- Checkpoint Firewall-1 firewall (gw)
- Content Technologies MailSweeper E-mail scanner (content).

For at skabe et overblik over forholdet mellem tidligere perioders hændelser og denne periodes hændelser, har jeg i graferne vist fordelingen af hændelser i denne periode sammen med et gennemsnit over de tidligere perioders hændelser.

Statistik vedr. FW-1 loggen

Der er i perioden blevet registreret **130.283.979** hændelser i loggen.

Nedenstående graf viser fordelingen af hændelser i perioden og et gennemsnit af samme for de foregående fire to-måneders perioder:

