Åtgärder efter intrång

Alla datorer som är uppkopplade på Umeå universitets datornät ska ha ett fullvärdigt skydd mot intrång. Erfarenheten har visat att de som försöker använda våra datorresurser (s.k. hackare) har blivit allt snabbare på att utnyttja de säkerhetshål som hittas. De program som används för att utnyttja andras datorer och också blivit alltmer sofistikerade. De säkerhetsuppdateringar som tillhandahålls av leverantörerna ska installeras snarast möjligt och helst bör en automatisk funktion finnas för denna hantering. Är en anställd t.ex. bortrest får inte en dator vara ansluten till internet utan att någon person är ansvarig för att eventuella säkerhetsuppdateringar installeras utan dröjsmål.

Leverantören av operativsystemet tillhandahåller ofta säkerhetsuppdateringar via någon form av nätbaserad funktion. Windows Update är ett exempel på en sådan funktion. Har man ytterligare programpaket installerade kan dessa applikationer kräva egna uppdateringar och som ansvarig för en dator är man skyldig att hålla reda på även sådana nödvändiga uppdateringar.

Idag förekommer ofta blandade attacker: D.v.s. det vi traditionellt tidigare har kallat för virus kan idag innehålla komponenter som såväl skickar skräppost via den egna datorn, söker efter nya datorer att infektera samtidigt som det öppnar en bakdörr och ge hackaren access och kontroll över datorn. Något som vid första anblicken ser ut som bara ett virusangrepp kan alltså i slutändan visa sig vara ett datorintrång där hackaren lagt upp en ftp-server på datorn för spridning av illegalt kopierad programvara.

Alla klientdatorer kan idag användas som servrar. Det finns flera olika typer av programvara som kan installeras för att ge dem en serverfunktionalitet som ftp, webb eller annat. Det vi avser med begreppet servrar i detta dokument är datorer som tillhandahåller generella tjänster som är den del av infrastrukturen.

1 Målgrupp

Alla användare som har datorer anslutna till Umeå universitets datornät.

2 Allmänt

Syftet med detta dokument är att beskriva hur man som anställd ska förfara om man upptäcker eller misstänker ett intrång på en dator. Med intrång avses inloggning av främmande person eller installation av främmande programvara.

3 Policy

Alla datorer som är anslutna till Umeå universitets datornät måste ha ett adekvat skydd mot intrång. Användaren ska uppträda på ett sådant sätt att ett intrång undviks. Användaren ska också vara uppmärksam på händelser som kan tyda på ett intrång i datorn.

ITS har IT-chefens befogenhet att vidta de åtgärder som behövs för att skydda nätet och begränsa skador både internt och externt.

4 Regler

Vid misstanke om intrång ska IRT, ITS (irt@umu.se) kontaktas utan dröjsmål.

För varje dator som är ansluten till Internet ska det finnas en ansvarig person som utan dröjsmål kan installera eventuella säkerhetsuppdateringar.

När intrång har konstaterats, och om inga andra omständigheter förekommer, är det viktigaste att förhindra fortsatt access för hackaren. Stäng inte av strömmen till datorn men koppla bort datorn ifrån nätverket. Starta inte om datorn innan man har undersökt intrånget. Informera prefekt och IRT om vad som har skett.

Under utredningen ska en dagbok föras, där det framkommer vilka aktiviteter som har vidtagits, av vem samt tid/datum och annan relevant information.

Allt tillgängligt material om intrånget ska sparas:
Loggar, hittade root-kit/programpaket och annat av intresse.
Bränn detta på CD/DVD eller kopiera till annat externt lagringsmedia (USB-sticka/hårddisk).
Försök att identifiera vilka aktiviteter som hackaren utfört på systemet.

Intrång som skett på en klientdator

I regel är det ingen större idé att försöka rensa en angripen klientdator. Risken finns att programvaror och andra filer fortfarande ligger kvar i systemet. Dessa kvarglömda filer kan komma att ställa till problem för användaren och eventuellt möjliggöra fortsatta intrång. Ominstallation rekommenderas därför:

- Monitorera systemet noga dagarna efter intrånget för att verifiera att aktiviteterna har upphört. Installera ev. en mjukvarubrandvägg, om inte detta finns sedan tidigare, för att ha kontroll över trafiken till/från systemet.
- Undersök liknande system efter spår av intrång och verifiera om dessa är rena eller också utsatta.
- Utred vilka rutiner som inte har fungerat.
- Utred om vi behöver ändra på gamla rutiner eller införa nya för att inte liknande intrång ska inträffa igen.
- Om intrånget har inneburit root-access eller admin-rättigheter måste användarnas lösenord bytas, då hackaren annars återigen kan ta sig in denna väg.
- Kontrollera om användaren har använt samma lösenord mot andra system. Om så är fallet ska även dessa lösenord bytas.
- Ta reda på om andra system är inblandade. Till exempel om hackaren använt detta system för att hoppa vidare till andra system inom det lokala nätet.

Systemet får inte sättas tillbaka på nätet förrän tillräckliga åtgärder har vidtagits.

Intrång som skett på en server

- Eliminera alla spår av hackaren från systemet. Installera om systemet om minsta tvekan finns om att inte alla hål har täppts till.
- Verifiera att inte information har ändrats på systemet. Om minsta tvekan råder om detta måste systemet installeras om från senast tagna back-up. Jämför mot back-up:ade filer.
- Stäng hackarens alla accessvägar till maskinen: Verifiera att inga nya användare har lagts upp genom att jämföra de filer som finns på backupen (tagna före intrånget). Detsamma gäller viktiga systemfiler och accesskontrollistor.
- Åtgärda de säkerhetsluckor som upptäckts, genom att:
  o Installera säkerhetsuppdateringar/patchar eller gör andra relevanta systemändringar för att förhindra upprepat intrång.
  o Se över brandväggsfiltren och andra säkerhetsrelaterade programvaror och se om dessa kan trimmas ytterligare.
  o Byt lösenord på admin-/root-lösenord och andra viktiga användare (även t.ex. SSL-nycklar). Om hackaren har haft root-access kan man förutsätta att denna också har tagit hand om lösenordsfilen och på sätt återigen kan koppla upp sig på systemet.
- Om intrånget har inneburit root-access eller admin-rättigheter måste användarnas lösenord bytas, då hackaren annars återigen kan ta sig in denna väg.
- Om någon form av sniffer har funnits installerade måste även byte ske av lösenord mot andra servar som man ansluter sig till/från aktuell maskin.
- Ta reda på om andra system är inblandade. Till exempel om hackaren använt det system för att hoppa vidare till andra system inom det lokala nätet.
- Kontakta andra systemadministratörer som kan vara berörda av intrånget.
- Följ upp intrånget genom att monitorera systemet noga dagarna efter intrånget för att verifiera att aktiviteterna har upphört. Installera ev. en mjukvarubrandvägg, om inte detta finns sedan tidigare, för att ha kontroll över trafiken till/från systemet.
- Undersök liknande system efter spår av intrång och verifiera om dessa är rena eller också utsatta. Utred vilka rutiner som inte har fungerat.
- Utred om vi behöver ändra på gamla rutiner eller införa nya för att inte liknande intrång ska inträffa igen.

Systemet får inte sättas tillbaka på nätet förrän tillräckliga åtgärder har vidtagits.

Vid intrång på servrar ska en utredning göras.

En skriftlig rapport ska skrivas för att dels dokumentera själva intrånget men också som en hjälp för att kunna förbättra våra interna rutiner.

I rapporten ska tydligt framgå:

- Systemets namn och IP-nummer.

- Operativsystem: Version och patchnivå/servicepack.
- Datum/tid för intrång och upptäckt.
- Beskrivning över hur intrånget upptäcktes.
- Beskrivning över hur intrånget har gått till. Installerade programvaror och andra aktiviteter.
- Aktiviteter som har utförts på systemet av systemansvariga med anledning av intrånget.
- Nedlagd tid.
- Vilka samtal som har förts och vad man kom fram till.
- Vilka som har meddelats i första läget.
- Vilka som har access till systemet.
- Vilka data som samlats in och var den finns lagrad.
- Vilken information som har skickats till olika parter (vad och till vem).
- Vilka andra system berörs av intrånget?
- Hur kunde intrånget ske?
- Vilka rutiner gick fel?
- Hur kan vi åtgärda så att det ej händer i framtiden? Nya eller ändrade rutiner?

Till rapporten ska dagbok och ev. CD-skiva med sparat material bifogas. En kopia av utredningen ska lämnas till prefekt, IRT och IT-chef.

5 Definitioner

Intrång: Angrepp av virus, trojaner, inloggning av främmande person eller installation av främmande programvara.

Hacker: Person som försöker få otillbörlig access till ett datorsystem.

Root-kit: Programvaror som installeras av hackare. Exempel på program som kan installeras är bakdörrar, fil-servrar, e-postserver för att skicka skräppost och program som stänger av den lokala brandväggen. Ett annat exempel är installation av scanningsprogram för att kunna använda den hackade datorn till att hitta andra sårbara datorer.

6 Se också

7 Revisionshistoria

Fastställt 2011-03-21/ Maria Tauson