Åtgärdsförslag

Angrepp via tjänsteleverantörer

Sammanfattning

Aktörer har på senare tid börjat angripa och ta sig in i tjänsteleverantörers IT-miljöer. Detta för att aktören i nästa steg ska kunna använda tjänsteleverantörernas nätverk som ett insteg till deras kunder. Denna rapport syftar till att belysa ett antal olika åtgärder som organisationer kan vidta för att upptäcka och försvåra angrepp via dessa kanaler.

Innehåll

1 Inledning

FRA vill genom denna rapport belysa ett antal skyddsåtgärder som en organisation kan vidta för att stärka sitt skydd mot ett angreppsätt som i media bland annat har benämnts ”Cloud Hopper”. Angreppsmetodiken har i praktiken inte med molntjänster i sig att göra, utan bygger snarare på att en angripare utnyttjar tjänsteleverantörers anslutningar till deras kunder för att på så vis få tillgång till deras IT-miljöer. Rapporten innehåller dels en beskrivning av hotet och dels konkreta åtgärdsförslag som förbättrar organisationers förmåga att upptäcka angrepp. Dessa åtgärder är uppdelade i en teknisk del samt en organisatorisk med åtgärder av mer strategisk karaktär.

De föreslagna tekniska åtgärderna bedöms vara genomförbara på kort till medellång sikt. Åtgärderna utgör sammantaget inte heller en komplett lista på lämpliga åtgärder och bör därför inte ses som ett fullgott skydd mot angrepp, dock skapar de enligt FRA en god grund. Tillämpligheten för olika åtgärder varierar dessutom mellan olika IT-miljöer.

2 Hotbild

Både svensk och utländsk media har rapporterat förekomsten av ett nytt generellt hot i form av en ny angreppsmetodik mot företag och myndigheter på den internationella arenan. Angriparens tillvägagångssätt är i korthet att nå sitt slutmål (olika företag och myndigheter) via en av ett antal vanligt förekommande tjänsteleverantörer, till vilka organisationen helt eller delvis outsourcat sin IT-drift.

De aktuella tjänsteleverantörerna angrips först och de olika nätverksuppkopplingar och behörigheter som dessa har till förfogande för kunna nå och distansadministrera sina kunders nätverk utnyttjas sedan av angriparen. När angriparen fått åtkomst till slutmålet via tjänsteleverantören kan denne tillskansa sig en direkt tillgång till miljön via dess normala internetanslutning, utan att behöva vara fortsatt beroende av att använda tjänsteleverantörens infrastruktur.

Sammanfattningsvis bör hotet hanteras som ett insiderhot, även om aktörer endast utnyttjar internt betrodda administratörskonton.

3 Detektion

Att upptäcka denna typ av angrepp kan vara mycket problematiskt då ingen skadlig kod eller avancerade attacker behöver användas mot slutmålet. Det initiala angreppet sker mot tjänsteleverantören, sedan utnyttjar angriparen de behörigheter och anslutningar som redan är upprättade mot slutmålets IT-miljö för legitim systemadministration. Inte sällan innebär detta att tjänsteleverantören och därmed angriparen får obegränsad åtkomst till IT-miljön. För tjänsteleverantörens kunder är det mycket svårt att avgöra om det är tjänsteleverantören eller angriparen som står bakom inloggningarna och anslutningarna, vilket gör att antivirus, IDS/IPS-system och andra typer av liknande säkerhetsprodukter i princip blir verkningslösa.

För att upptäcka om man blivit utsatt för denna typ av angrepp krävs att åtgärder redan vidtagits för att spåra och logga aktivitet i IT-miljön, samt lagra detta på ett centraliserat och säkert sätt. Med säkert menas att man vidtagit åtgärder som förhindrar manipulation av loggar i efterhand. Detta blir naturligtvis en särskilt svår uppgift om det är just denna typ av infrastruktur som har upphandlats och som en extern tjänsteleverantör ska tillhandahålla.

FRA rekommenderar att beställare av IT-tjänster ber leverantören att redovisa de ärenden som det senaste kvartalet har resulterat i att någon åtkomst till den egna IT-miljön har skett. Detta korreleras sedan mot egna loggar i syfte att se om det finns inloggningar och anslutningar som inte överensstämmer med ett av tjänsteleverantören redovisat ärende. Om inte alla förekomster av konstaterad åtkomst kan korreleras mot berättigad åtkomst, kopplade till riktiga ärenden, måste dessa händelser utredas ytterligare. Börja med den åtkomst som har skett mot de system som innehåller den mest skyddsvärda informationen. Om tjänsteleverantören uppvisar oförmåga att skyndsamt ta fram den efterfrågade informationen är detta att ses som en brist i sig.

4 Föreslagna förebyggande och skadebegränsande åtgärder

I detta avsnitt ger FRA praktiska råd gällande åtgärder som kan övervägas av organisationer som vill försvåra den beskrivna angreppstypen. Råden är uppdelade på teknisk nivå samt organisatorisk nivå.

4.1 Tekniska åtgärder – loggning och spårbarhet

Det är viktigt att förstå att det normalt är mycket svårt att upptäcka anomalier på ett internt nätverk eller att i detalj kunna avgöra vad som händer eller har hänt med mindre än att man har en god loggning och spårbarhet.

En stor del av de tekniska åtgärderna syftar därför i grund och botten till att skapa förutsättningar att övervaka aktiviteter i den interna infrastrukturen, i synnerhet administrativa sådana och sådana som initieras över en extern förbindelse via en tjänsteleverantör. Övervakning kan användas dels för att upptäcka avvikelser som indikerar att miljön är kompromitterad och dels för att kunna gå tillbaks i tid och se vad som hänt i miljön, till exempel för att genomföra en menbedömning. En annan fördel med att etablera en väl fungerande övervakning av interna administrativa åtgärder är att ge allmänt stöd för kvalitetssäkring av tjänsteleverantörens produkt.

För att kunna övervaka administrativ åtkomst på ett tillfredsställande sätt bör tjänsteleverantören vara tvungen att använda en mellanliggande ”hoppserver” för att sedan ansluta vidare till sin kunds infrastruktur. Leverantören bör alltså inte ha möjlighet att direkt ansluta från sitt nätverk in till kundens olika servrar. VPN bör användas av tjänsteleverantören, men detta bör alltså termineras på hoppservern. Viktigt är att hoppservrarna inte ska administreras av tjänsteleverantören själv, utan av kundens egen personal och/eller en från tjänsteleverantören oberoende inhyrd part.

Nedan ges rekommendationer gällande övervakning av fjärradministrationen:

- För hoppservrar ska strikt nätverksfiltrering och loggning för både tillåtna och icke tillåtna nätverksflöden tillämpas. Utökad loggning av aktiviteter på andra servrar som används av tjänsteleverantören bör dessutom införas.

- Inga former av trafikflöden får tillåtas passera en hoppserver utan mellanliggande terminering.

- En central logghantering bör finnas, i synnerhet gällande system som används för att administrera IT-miljön såsom hoppservrar. De insamlade loggarna behöver sedan kontinuerligt analyseras för att obehöriga inloggningar och avvikelser, exempelvis oväntat arbete utanför ordinarie kontorstid, snabbt kan upptäckas.

- Centraliserad logganalys och detektion ska i grunden vara automatiserad med möjlighet till manuell analys vid behov. För att förhindra manipulation och utslagning av de centrala loggarna bör den centrala loggfunktionen isoleras och administreras via betrodda och fysiskt dedikerade arbetsstationer.

- Insamlade loggar bör sparas även på längre sikt för att kunna ge stöd vid incidenthantering och menbedömning. Loggarna kan ge ovärderliga ledtrådar i fall där en angripare haft förmåga redan i tidigare skede, innan incidenten detekterades.

- Lösningar för inspelning av nätverkstrafik relaterad till systemadministration bör dessutom övervägas. Även denna måste säkras upp så att en angripare inte kan tillskansa sig informationen i den inspelade trafiken eller modifiera denna.

- Om så är möjligt och relevant för utformningen av hoppservern, inför loggning av hur mycket trafik som passerar genom hoppservern. Om endast enkel systemadministration utförs via denna server kan flöde av större datamänger över hoppservern tyda på att data exfiltreras.

4.2 Tekniska åtgärder – autentisering och åtkomststyrning

En annan central del i de tekniska åtgärderna är att förstärka autentiseringsmetoder som används för administrativ åtkomst till miljön. Nedan ges rekommendationer gällande autentisering och åtkomststyrning:

- Kräv att tjänsteleverantörer anskaffar kundspecifik utrustning och lösningar för administration som alltid håller den egna interna infrastrukturen frånkopplad från tjänsteleverantörens. Datorer på vilka systemadministration utförs ska inte användas för andra syften, exempelvis att läsa e-post eller surfa på internet.

- Hoppservrar bör använda starka autentiseringsmetoder som är oberoende gentemot såväl den interna miljön som tjänsteleverantörens infrastrukturer. Tjänsteleverantören ska alltså i steg 1 autentisera mot hoppservern. I steg 2 autentiserar tjänsteleverantören vidare från hoppservern mot de system som ska administreras. Åtkomst till hoppservern ska alltid ske med flerfaktorsautentisering, inte bara lösenord eller mjukt certifikat.

- Byt lösenord på alla konton som har administrativa rättigheter och säkerställ att de byts med jämna mellanrum.

- Genomför automatisk och regelbunden inventering av konton som inte loggat in på länge, för att avgöra om dessa går att avaktivera.

- Endast personliga konton ska användas vid administration av system. Generella gruppkonton eller inbyggda systemkonton bör inte användas.

- Systemadministration ska endast kunna ske med flerfaktorsautentisering.

- Administratörer bör delas in i olika roller och endast medges tillgång till systemen vid behov.

- Administratörsroller bör endast ges åtkomst till de system som rollen innefattar vilket säkerställs med ändamålsenlig segmentering och filtrering i nätverket.

- Slutligen bör det eftersträvas att tjänsteleverantörer, där möjligt, endast ges åtkomst till kundens miljö vid behov och endast till delar den behöver åtkomst till vilket säkerställs med ändamålsenlig segmentering i nätverket. Det kan till exempel ske i form av inkoppling efter telefonkontakt.

Alla åtgärder i miljön bör hanteras inom en kontrollerad förändringshanteringsprocess. Om verksamheten så tillåter kan tjänsteleverantören tekniskt helt förhindras från att fjärransluta till miljön (typiskt hoppservern) utan att en föregående överenskommelse med en intern kontaktperson finns. Denna kontaktperson ska då tekniskt kunna aktivera

fjärråtkomstmöjligheten under ett för det specifika uppdraget lämpligt tidsfönster. Tjänsteleverantörens konton kan också begränsas till att endast vara aktiva under sådana tidsperioder.

4.3 Organisatoriska åtgärder

En grundproblematik som typiskt ökar en organisations utsatthet för angrepp av det beskrivna slaget, är den interna säkerhetsmässiga kompetensförlust som ofta är ett delresultat av en outsourcingprocess. Organisationen önskar i regel att minimera den egna IT-avdelningen och i stället upphandla många av dess roller, exempelvis IT-säkerhetsspecialister, från en extern part. Den externa parten blir inte sällan samma företag som senare även ska hantera IT-driften.

Att behålla egen nyckelpersonal, framför allt för kravställning och säkerhetsstyrning är enligt FRA:s uppfattning av mycket stort värde för en organisation. Sådan personal har både teknisk kunskap och erforderlig verksamhetskunskap, tillika sannolikt större önskan att organisationen ska ha en välfungerande IT-miljö. Detta innebär att de kan utgöra en verklig motpart när tjänster från leverantörer sedan ska kravställas, avropas och kvalitetssäkras.

Nedan ges rekommendationer gällande organisatoriska åtgärder:

- Engagera och informera organisationens ledning i problematiken kring denna hotbild och understryk dess potentiella konsekvenser samt ledningens ansvar för dessa.

- Utvärdera noga vilka system som är lämpliga att lägga ut på entreprenad och vilka som bör behållas internt. Detsamma gäller vilka system och delar av IT-miljön som drift lämpar sig för outsourcing till tjänsteleverantör och vilka delar där drift och loggning bör ske av egen personal. Säkerställ att tjänsteleverantörens tilldelade konton och accesser inte kan nå de delar och system som bibehålls för intern drift.

- Behåll och rekrytera egen nyckelpersonal för kravställning och styrning av IT-säkerhet. Undvik att använda IT-säkerhetstjänster som levereras av samma företag som hanterar IT-driften.

- Kvalitetssäkra all tidigare och ny säkerhetskravställning mot tjänsteleverantörer med hjälp av egna och/eller, i förhållande till leverantören, oberoende inhyrda säkerhetsexperter. Säkerhetskrav ska vara tydliga, spetsiga och lämna en liten tolkningsmån.

- Säkerställ att leverantörens arbetsformer i praktiken är förenliga med gällande lagar och bestämmelser. Sker exempelvis arbete alltid inom svensk jurisdiktion, med personal som är erforderligt säkerhetsklassad om så är grundkravet? Håller avtalen i dessa avseenden och vad händer exempelvis om tjänsteleverantörens ägandeförhållanden förändras? Säkerställ att avtal kan sägas upp utan förbehåll om förändringar påverkar säkerheten.

- Säkerställ att övervakning av leverantörers åtgärder i IT-miljön löpande kan ske med egna och/eller med i förhållande till leverantören oberoende inhyrda säkerhetsexperter. Detta krav ska finnas med i avtalet med tjänsteleverantören och bör åberopas med återkommande intervall.

- Sträva efter att ha en egen förmåga att upptäcka och initiera utredningar av IT-incidenter, exempelvis genom att ha en egen operativ nätverksövervakning och resurser insatta i incidentutredning. Om sådana förmågor avropas från leverantör bör detta komma från en annan leverantör än den som sköter IT-driften.

Organisationer rekommenderas vidare att se över sin informationsklassning och att identifiera de viktigaste informationstillgångarna i den interna IT-miljön. En angripare som på det beskrivna sättet tillskansar sig full administrativ behörighet till en miljö som tillåter fjärråtkomst har möjlighet att kunna exfiltrera godtycklig intern information ur alla i någon mening nätverksanslutna system. Särskilt känslig information som idag lagras i den ordinarie IT-miljön men inte behöver eller borde lagras i det interna nätverket kan med fördel separeras ut till system som inte är direkt anslutna till den ordinarie miljön. Detta medför att viss kontroll kan garanteras när det gäller åtkomst till denna typ av information även om den interna miljön skulle bli kompromitterad på det beskrivna sättet.