Myndigheten för samhällsskydd och beredskap

PM

Datum
2020-06-09

Ärendenr
MSB2020-08976-1

Avdelningen för cybersäkerhet och säkra kommunikationer

Öka motståndskraften mot ransomware

Rekommendationer riktade till it-personal, beslutsfattare respektive användare inom hälso- och sjukvårdssektorn.

Innehåll

Inledning

Det här dokumentet har tagits fram i samverkan mellan fyra myndigheter – Försvarets radioanstalt, Myndigheten för samhällsskydd och beredskap, Polismyndigheten och Säkerhetspolisen – och innehåller rekommendationer gällande hur organisationer inom hälso- och sjukvårdssektorn kan öka motståndskraften mot ransomware, även kallad utpressningstrojaner. Dessutom beskrivs hur spår av intrång kan upptäckas i it-miljön samt konkreta råd om vad som behöver göras för att åstadkomma en snabb återställning av verksamheten när angreppet är ett faktum. Vidare i detta dokument kommer den engelska benämningen ”ransomware” att användas.

Dokumentet ska ses som ett underlag och stöd där respektive organisation/verksamhet inom hälso- och sjukvårdssektorn kan använda innehållet för riskanalyser, beslutsunderlag, utbildning och kommunikation på det sätt som bedöms vara lämpligt för verksamheten. Exempelvis kan ytterligare målgruppsanpassning av budskapen således behöva göras.

Målgruppen är främst alla ansvariga för it-infrastruktur inom hälso- och sjukvårdsverksamhet men en del av materialet riktar sig specifikt till it-tekniker/ systemadministratörer inom densamma. Den tredje delen är råd som riktar sig till användare av verksamhetens it-system.

Hotbilden

Ett angrepp av ransomware kan innebära att hela eller delar av en verksamhets it-system med dess information blir krypterad och inte är tillgänglig för personalen. Detta kallas ofta för ransomware, från engelskans ”ransom” (lösensumma) och ”software” (mjukvara). Därmed hoppas angriparna på att den utsatta organisationen ska betala en lösensumma för att få tillgång till dekrypteringsnyckeln och därmed få tillbaka den förlorade informationen. I många fall stjäls även information och angriparna hotar med att publicera den känsliga informationen om en lösensumma inte betalas. Som verksamhetsansvarig behöver du ha en uppfattning om vilka konsekvenser ett sådant angrepp skulle få för både verksamheten och patientsäkerheten.

Precis som inom andra sektorer i samhället har även hälso- och sjukvårdssektorn moderniserats med innovativa it-lösningar såsom uppkopplad medicinteknisk utrustning eller att olika system med vårdregister är sammankopplade och uppkopplade till internet. Denna digitalisering innebär att vi både är mer beroende av fungerande it-system men också att systemen är mycket mer exponerade. Det här innebär också stora utmaningar för säkerhetsansvariga när digitaliseringstakten i vissa fall har gått snabbare än säkerhetsarbetet i it-miljön.

Varför denna informationsinsats nu?

Under pågående covid-19-pandemi har flera rapporter från internationella instanser inkommit som belyser att organisationer inom hälso- och sjukvårdssektorn visat sig vara särskilt attraktiva mål för cyberangrepp. En anledning till detta kan vara att medicinsk data är värderad mycket högt och kan användas för utpressning. Kriminella kalkylerar med lönsamhet när tillräckligt många väljer att betala lösensumman, särskilt om krypterad data

inte är möjlig att återskapa på något annat sätt, är känslig eller att människors liv och hälsa står på spel. Exempelvis angreps Europas största privata sjukhusverksamhet Fresenius i maj av ransomware. Efter angreppet fanns stulen patientdata från företaget tillgänglig på internet innehållande medicinsk data och identifierbara personuppgifter från patienterna.

I Sverige har både offentlig och privat verksamhet drabbats av ransomware det senaste året. När sjukvården är under ett oerhört påfrestat läge, där personalen belastas hårt för att ta hand om sjuka, skulle ett sådant angrepp slå hårt. Risken att detta kan inträffa i Sverige går inte att bortse från. Under ett krisläge, som den pågående covid-19-pandemin innebär, är det synnerligen viktigt att följa de dagliga it-säkerhetsprocesser och rutiner som är etablerade. Sjukhusens it-personal bör inte distraheras utan tillåtas att fokusera på det löpande underhåll som är nödvändigt för att skydda systemen.

Åtgärder när ransomware är ett faktum

Betala aldrig kravet på lösensumma. Det finns inga garantier att system återställs eller filer dekrypteras.

I korthet sammanfattas här några övergripande råd över hur en incident med ransomware bör hanteras:

- Isolera smittade enheter.
- Anmäl händelsen i ett tidigt skede, t.ex. polisanmäl, incidentrapportera till myndigheter efter bedömning av incidentens art, enligt NIS-direktivet eller enligt säkerhetsskyddslagen för säkerhetskänslig verksamhet.
- Vid behov, sök stöd i incidenthanteringen av myndigheter, säkerhetsföretag etc.
    - MSB/CERT-SE ger stöd och råd till drabbade vid it-incidenter inom såväl offentliga som privata organisationer.
- Säkerställ i er utredning att angreppet är åtgärdat och att angriparen inte har fortsatt tillgång till it-miljön genom behörigheter och/eller skadlig kod i systemet.
- Innan återställning av säkerhetskopior sker, säkerställ att kopiorna inte också har drabbats.

Förebyggande åtgärder

Det går inte att helt skydda sig från angrepp, men förebyggande åtgärder som kontinuerligt it-säkerhetsarbete med bra rutiner för säkerhetskopiering och återställning samt att utbilda personalen, underlättar hanteringen och begränsar skadan. Möjligheten att snabbt kunna återställa it-miljön så att verksamheten kan återgå till normalitet och hålla nere kostnaderna för hanteringen av angreppet kan göra betydande skillnad.

Rekommendationerna består av följande delar:

1. Råd till tekniker och systemadministratörer som sköter drift och underhåll av it-system
2. Råd till beslutsfattare och ansvariga för verksamhetens it-infrastruktur
3. Råd riktat till användare av verksamhetens it-system

Råd till tekniker och systemadministratörer som sköter driften och underhåll av it-system

Här följer konkreta åtgärder som riktar sig till it-tekniker/-systemadministratörer inom hälso- och sjukvårdsenheter, vilka bör genomföras i syfte att skydda it-miljön från intrång och skydda patientdata. Åtgärderna som listas nedan kan ses som en checklista och är sådant som behöver införas snarast, utan att kräva omfattande investeringar eller utvecklingsarbete.

Jobba för en god säkerhetsmedvetenhet

Informera och utbilda organisationens användare om förekomsten av olika typer av phishing, även kallat nätfiske. Utbilda dem i att göra en rimlighetsbedömning innan de klickar på länkar eller bifogade filer i ett e-postmeddelande (se avsnittet *Råd riktat till användare av verksamhetens it-system*).

Översyn av säkerhetslösningar

- Gör en översyn av de säkerhetslösningar och tjänster som organisationen nyttjar, och aktivera de säkerhetsfunktioner som finns tillgängliga. Sådana lösningar kan exempelvis vara:
  - Aktivera antivirus och då även på servrar.
  - Tillåt endast att godkända program exekveras exempelvis med hjälp av exempelvis Applocker (i Windows-miljöer).
  - Aktivera SPF och DMARC-policy i e-postsystemet för att försvåra för angripare att imitera legitima användare.
  - Implementera lösningar som kan identifiera och blockera skadliga länkar och filer i e-post samt en lösning som kan blockera åtkomst till skadliga hemsidor och IP-adresser för användarna.
- Aktivera flerfaktorsautentisering där det är möjligt. Detta förhindrar en angripare att återanvända stulna inloggningsuppgifter, vilket är särskilt viktigt för system för fjärranslutning.

Ta regelbundna säkerhetskopior

- Skapa säkerhetskopior av data och systemkonfigurationer/-inställningar.
- Testa säkerhetskopiorna och återställningsrutiner med jämna mellanrum.
- Säkra era kopior genom att lagra dessa offline och offsite för att minska risken att de förstörs digitalt eller fysiskt.

Härda er it-miljö

- Uppdatera operativsystem och mjukvaror till den senaste versionen, så de överensstämmer med leverantörens rekommendationer, i synnerhet för de system som är exponerade mot internet.
- Använd endast säkra och i första hand krypterade protokoll. Inaktivera tjänster och protokoll som inte behövs eller används.

- Undvik att exponera RDP mot internet. Flytta hellre in sådan fjärråtkomst bakom en VPN-anslutning.
- Minska exponeringen mot internet. Endast servrar som levererar publika tjänster bör vara åtkomliga via internet och bara på de portar som krävs för ändamålet. Övriga portar som inte behöver vara åtkomliga utanför det lokala nätverket ska blockeras.
- Använd säkra programinställningar, särskilt för e-post, ordbehandlare och webbläsare. Utgå ifrån leverantörers egna härdningsguider för säkrande av it-miljön
- Förhindra att oönskade makron kan exekveras, genom att centralt styra inställningarna så att inte användaren själv tillåts välja lägre säkerhetsnivå.
- Aktivera den lokala brandväggen i både klienter och servrar.
- Håll regelverket uppdaterat och revidera kontinuerligt.
- Sträva mot ett segmenterat nätverk, med både fysisk och logisk separation.
- Se till att SMB (port 445/tcp) är blockerat för de system och klienter som inte behöver denna tjänst.

Begränsa behörigheter

- Använd inte gemensamma inloggningsuppgifter. För spårbarhet ska varje användare och administratör använda ett personligt konto.
- Använd inte administratörskonton till vardagliga sysslor, t.ex. läsa e-post eller surfa.
- Ge inte användare fler behörigheter än de strikt behöver.
- Inaktivera och rensa behörigheter på oanvända konton, missa inte grupptillhörigheter.
- Minska antalet permanenta medlemmar i högpriviligierade grupper som t.ex. Domain Admins till ett absolut minimum.

Övervaka

En god inblick i it-miljön är avgörande för förmågan att upptäcka cyberangrepp eller andra anomalier. Ta hjälp av er lösning för övervakning i syfte att få en uppfattning om vad som motsvarar organisationens normalläge. Att känna sin egen organisation är en förutsättning för att kunna tillhandahålla ett fullgott skydd för it-miljön.

Alla varningar och anomalier som rapporteras från säkerhetsprodukter bör utredas noggrant. Konfigurera därför er övervakning så att de larm och varningar som ges går att agera effektivt på.

Det är viktigt att spara loggar under en lång tidsperiod eftersom det är vanligt att det initiala intrånget har skett relativt långt innan angreppet blir synligt när filer börjar krypteras. Att genom loggar kunna följa intrånget är viktigt för att kunna genomföra en lyckad utredning och också minimera skadan.

Övervaka särskilt:

- Era lösningar för fjärråtkomst (t.ex. RDP).
- Nätverkstrafik, både intern och extern (inkommande/utgående) trafik, bör inspekteras.
- Förändringar och tömning av säkerhetsloggar, samt användning av PowerShell.
- Nyttjande av administratörskonton.
- Förändringar av behörigheter.
- Anslutningar mot tredjepartsleverantörer, samarbetspartners eller andra externa aktörer som möjligtvis har en lägre säkerhetsnivå och därmed gör er organisation sårbar.

Råd till beslutsfattare och ansvariga för verksamhetens it-infrastruktur

För att bygga upp motståndskraft mot angrepp och intrång i it-miljön och system krävs ett systematiskt it-säkerhetsarbete och en långsiktig plan som omfattar allt från nödvändiga investeringar till kontinuitetshantering.[1] Att ha en god planering för hur verksamheten ska fungera på en tolerabel nivå oavsett störning, är en bra grund. Här följer några råd till beslutsfattare och ansvariga för verksamhetens it-infrastruktur.

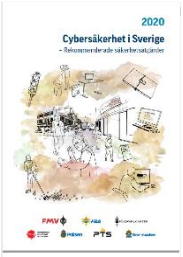
Ge it-personal goda förutsättningar att göra sitta jobb

Vid kriser eller i samband med andra långvariga störningar, väljer många verksamheter att inte genomföra utveckling och underhållsarbeten i normal omfattning. De som genomför angrepp på verksamheters it-system utvecklar kontinuerligt sina tekniker och utnyttjar nytillkomna sårbarheter. Att under längre perioder välja att *inte* genomföra säkerhetsuppdateringar innebär alltså en stor risk. Det är därför viktigt att fullfölja sitt säkerhetsarbete och genomföra strategiska beslut och investeringar så att it-administratörer vidare ska kunna genomföra förebyggande åtgärder. Det är viktigt att fortsätta att prioritera säkerhetsunderhåll av it-miljön trots att andra delar i verksamheten kan vilja begränsa arbeten som kan innebära vissa avbrott i tjänsten. Sådana arbeten måste dock planeras noggrant i syfte att minimera påverkan.

Informera om problemet

Låt medarbetare få information och gör dem medvetna om riskerna med ransomware och att just hälso- och sjukvårdssektorn är särskilt utsatt. En av de vanligaste kanalerna för att sprida skadlig kod är genom ”bifogad fil” eller genom att få användaren att klicka på länkar som leder till webbsidor där skadlig kod finns. Utbilda och öva medarbetarna i att vara uppmärksamma på misstänkt e-post.

Inför rekommenderade säkerhetsåtgärder



Genom att höja den generella säkerhetsnivån ökar motståndskraften mot många cyberhot. I rapporten *Cybersäkerhet i Sverige – rekommenderade säkerhetsåtgärder*[2] har flera myndigheter i samverkan lämnat gemensamma råd om vilka åtgärder som rekommenderas att införa. Dessa råd ersätter inte ett systematiskt säkerhetsarbete utan utgör ett stöd i arbetet med att prioritera vad som behöver göras.

Planera och öva för helt eller delvis bortfall av it-miljön

Håll planen för incidenthantering och kontinuitetsplanen uppdaterad samt öva så att organisationen både har kunskap och färdighet för att hantera incidenter. Genom att öva kommer hanteringen av incidenten att gå bättre i en kritisk situation och minimera risken att personal frångår rutinerna eller tar genvägar som kan öka riskerna och göra verksamheten mer sårbar. Vid ett lyckat angrepp av ransomware kan det ta veckor eller

[1] https://www.msb.se/kontinuitetshantering
[2] https://www.msb.se/contentassets/fe72c449466e4017bd76787762ab9dc5/rapport-cybersakerhet-i-sverige-2020---rekommenderade-sakerhetsatgarder.pdf

månader att återfå kontroll över it-miljön. Planera för att minska den påverkan ett så långt bortfall kan ha på verksamheten.

Skapa också en planering för att kunna bygga upp behörighetskatalogen (AD) från början. Vid ett intrång är det näst intill omöjligt att garantera att angriparen inte längre har åtkomst till systemet. Därmed kan behörighetskatalogen behöva byggas upp på nytt.

Säkerställ att medarbetare har tillräcklig utbildning gällande säkerhet för att kunna agera rätt.

Råd riktat till användare av verksamhetens it-system

Så kan du bidra till att skydda it-miljö och stärka patientsäkerheten

Du som använder verksamhetens it-system är också en viktig del i arbetet med att skydda dem, tillsammans med de tekniska skydd som er it-förvaltning har satt upp. Via ett tillsynes vanligt och oskyldigt e-postmeddelande kan ett datorvirus komma in och i förlängningen leda till att it-systemen för hela organisationen slutar att fungera.

Tänk efter innan du klickar!

Ibland kan det gå fort och ibland måste det gå fort för att säkerställa god patientsäkerhet. Alla måste vi ändå ta oss tid att tänka efter innan vi klickar och öppnar e-post med tillhörande filer. Genom att ställa dig dessa frågor kan du göra stor skillnad för att skydda verksamhetens it-miljö:

1. Förväntar jag mig ett e-postmeddelande från den personen/avsändaren vid den här tidpunkten? *Typiskt för bedrägliga meddelanden är att ärendet är brådskande, ett tidsbegränsat erbjudande eller "för bra för att vara sant".*
2. Är ärendet och meddelandet rimligt/förväntat? *Titta på språket och annat som avviker från t,ex. en rutin.*
3. Kontrollera avsändaren, ser adressen korrekt ut, borde den avsändaren skicka detta? *Obs! Tänk på att ett e-postkonto kan vara kapat vilket gör föregående frågor viktiga i bedömningen.*
4. Innehåller meddelandet en länk eller bifogad fil? *Kontrollera om länken eller filen verkar rimlig, eller ser konstig ut, eller innehåller ett namn som försöker efterlikna någon annan organisation. Var uppmärksam på om du länkas vidare till andra dokument eller sidor.*
5. Får du ett meddelande där du uppmanas att ange eller ändra dina inloggningsuppgifter? *Många angripare försöker imitera inloggningssidor för tjänster såsom Microsoft Office 365, Gmail etc.*
6. Uppmanas du avaktivera skyddad vy eller aktivera makron? *Datorvirus kan gömmas i t.ex. makron. Säkerhetsvarningar som t.ex. handlar om att aktivera makron ska du vara extra försiktig med och först verifiera med avsändaren att dokumentet är riktigt.*

Ta kontakt och rapportera!

Om du känner osäkerhet efter att du ställt dig ovanstående frågor eller tycker att det mottagna e-postmeddelandet verkar misstänkt, bör du ta det på allvar och göra någon eller båda av följande:

- Verifiera med avsändaren via andra kanaler, t.ex. genom att ringa upp och fråga avsändaren som skickat e-postmeddelandet och försäkra dig om dess riktighet.
- Kontakta, rapportera och sök stöd av it-avdelning för att bedöma e-postmeddelandet.

Myndigheten för samhällsskydd och beredskap

Postadress: 651 81 Karlstad
Telefon: 0771-240 240
Fax: 010-240 56 00
registrator@msb.se
www.msb.se
Org.nr: 202100-5984

Kontaktuppgifter

Vid frågor om innehållet, eller om råd och stöd vid it-incidenter, kontakta MSB/CERT-SE

e-post: cert@cert.se

telefon: 010-240 40 40

Myndigheten för samhällsskydd och beredskap

Postadress: 651 81 Karlstad
Telefon: 0771-240 240
Fax: 010-240 56 00
registrator@msb.se
www.msb.se
Org.nr: 202100-5984