Polisen

Polismyndighetens allmänna råd kring IT-säkerhetsåtgärder

IT-säkerhetsenheten

Inledning

De allra flesta tekniska plattformar och it-stöd som används i vårt samhälle idag, oavsett om de återfinns inom näringslivet eller inom offentliga sektorn, har på något sätt ett beroende till eller är uppkopplade mot internet. Denna samhällsutveckling har medfört att de allra flesta verksamheter och organisationer automatiskt blir föremål för de it-relaterade hot som vår moderna teknik och internet har gett upphov till. Förmågan att kunna skydda sin verksamhet mot dessa it-relaterade hot har därför blivit alltmer viktigt.

Polismyndigheten har under de senaste åren konstaterat att antalet anmälda brott som kan relateras till dataintrång har ökat. Polismyndigheten har under det brottsutredande arbetet även kunnat konstatera att genomförandet av intrången blivit allt mer komplext ur ett tekniskt perspektiv.

Som en del i det brottsförebyggande arbetet har Polismyndigheten valt att sammanställa en förteckning med IT-säkerhetsåtgärder till stöd för de verksamheter som är föremål för den generella hotbild som en Internetansluten IT-infrastruktur medför.

Målet är att bidra till en effektiv basnivå av IT-säkerhet.

Målgrupp

- De primära målgrupperna för dessa allmänna råd är IT-säkerhetsspecialister och IT-tekniker

- Sekundära målgrupper är it-chefer, it-säkerhetschefer, projektledare för it-säkerhetsprojekt etcetera.

Omfattning och avgränsning

- De skyddsåtgärder som beskrivs i dessa allmänna råd är uppdelade utifrån följande tre övergripande kategorier:
  - Åtgärder som förebygger att skadlig kod kommer in i it-miljön och får fotfäste
  - Åtgärder för att begränsa konsekvenserna av ett intrång
  - Åtgärder för att i tid upptäcka och hantera intrång

- Dessa skyddsåtgärder ska inte ses som en komplett lista över alla it-säkerhetsåtgärder som behövs för att skydda sin verksamhet mot avancerade hotaktörer. I övrigt har Polismyndigheten i dessa råd inte tagit hänsyn till de krav på it-säkerhetsåtgärder som återfinns i specifika författningar såsom Föreskrifter och allmänna råd om statliga myndigheters informationssäkerhet (MSBFS 2016:1), Säkerhetsskyddslagen (2018:585) med flera.

Förklaringar av de olika begreppen som används i dessa råd

Hur effektiv är åtgärden?	Mycket effektiv = åtgärden försvårar för ett brett spektrum av intrångsmetoder från att fungera. Angriparen måste använda speciallösningar för att kringgå åtgärden.
	Effektiv = åtgärden är ett effektivt komplement till att minska angreppsytan ytterligare och därmed skapa fler hinder som en angripare måste ha förmåga att ta sig förbi.
Åtgärd	En it-säkerhetsåtgärd kan antingen förebygga intrång, minska en angripares möjligheter att ”röra sig” i it-miljön eller försvåra för angriparen att inte bli upptäckt.
Beskrivning	En mer detaljerad beskrivning av varför åtgärden är effektiv och/eller en beskrivning av mer avancerade implementationer.
Potentiell användarpåverkan	Hög = Sannolikt att åtgärden orsakar en negativ påverkan för en begränsad grupp användare, i de flesta fall it-teknisk personal. Påverkan kan även avse motstånd mot åtgärden, exempelvis borttagning av onödiga administratörsrättigheter. Medel = Mindre sannolikt att åtgärden skapar ett motstånd eller orsakar negativ påverkan för användare. Beror på den berörda verksamheten och dess unika förhållanden. Låg = Åtgärden ska i normala fall inte påverka användarna negativt
Resursåtgång (personal, tid, kostnader för mjuk- och hårdvara)	Hög = åtgärden kräver tillgång till specialistkunskaper som innebär höga personalkostnader samt investeringar i hård- och mjukvara Medel = åtgärden kräver ett organiserat och kontinuerligt arbete med drift och förvaltning av säkerhetsfunktionen men är inte särskilt tidskrävande. Låg = Åtgärden kräver endast en begränsad resursåtgång i form av tid, investeringar och personalkostnader. Oftast en åtgärd som kan implementeras en gång och därefter endast kräver minimal förvaltning.

Sammanfattning av de effektivaste åtgärderna

Stoppa skadlig kod

- [ ] Applikationskontroll
- [ ] Säkerhetsuppdatera applikationer som är exponerade
- [ ] Konfigurera makro-inställningar i Microsoft Office
- [ ] Aktivera skyddsfunktioner i Windows Exploit Guard

Begränsa omfattningen av intrång

- [ ] Var restriktiv med användningen av administratörskonton
- [ ] Installera säkerhetsuppdateringar för operativsystemet
- [ ] Använd stark autentisering vid inloggning i klientdatorer och servrar
- [ ] Avaktivera lokala administratörskonton
- [ ] Använd Microsoft Credential Guard eller motsvarande funktion för andra operativsystem
- [ ] Begränsa vilka processer som får kommunicera ut mot Internet
- [ ] Ha effektiv detektionsförmåga genom logganalys av operativsystemsnära loggdata och analys av utgående kommunikation

Återställ tillgängligheten till information och IT-system

- [ ] Daglig säkerhetskopiering

ÅTGÄRDER SOM FÖREBYGGER ATT SKADLIG KOD KOMMER IN I IT-MILJÖN OCH FÅR FOTFÄSTE

Applikationskontroll

Hur effektiv är åtgärden?	Beskrivning	Potentiell användarpåverkan	Resursåtgång
Mycket effektiv	Vitlistning av applikationer säkerställer att endast godkänd programvara får köras (inklusive .exe, DLL, script m m). För att motverka att obehörig och otillåten programvara eller skript, inklusive skadlig kod körs i organisationens klientdatorer och servrar behöver en funktion för applikations-vitlistning vara implementerad. Exempel på produkter med vitlistningsfunktionalitet är Microsoft AppLocker och Apple Gatekeeper. Rätt införd är denna åtgärd ett mycket effektivt skydd mot att skadlig kod får fotfäste.	Medel	Medel

Installera säkerhetsuppdateringar för exponerade applikationer

Hur effektiv är åtgärden?	Beskrivning	Potentiell användarpåverkan	Resursåtgång
Mycket effektiv	Installera säkerhetsuppdateringar för applikationer som används vid bearbetning av innehåll från Internet så fort som möjligt. Prioritera att uppdatera webbläsare, PDF-läsare, Microsoft Office-applikationer, Java, Adobe Flash etcetera.	Medel	Medel

Konfigurera makro-inställningar i Microsoft Office

Hur effektiv är åtgärden?	Beskrivning	Potentiell användarpåverkan	Resursåtgång
Mycket effektiv	Konfigurera Microsoft Office makro-inställningar för att blockera inbyggda makrofunktioner i dokument från obetrodda källor. Om det inte är möjligt att blockera utan stor negativ verksamhetspåverkan – inaktivera makron så att användaren får en varningstext om att det är riskabelt att aktivera makron i bilagor som kommer från externa avsändare. Mer avancerade åtgärder: • Tillåt makron att endast köra från betrodda kataloger med begränsade skrivrättigheter i användarnas datorer. • Tillåt endast makron som är digitalt signerade med ett giltigt certifikat från att köra. • Blockera allra helst makron som kommer från externa källor. • Använd ”betrodda platser” i klienten där makron får köra. • Använd Windows Defender Exploit Guard och Attack Surface Reduction för att minimera farliga beteenden från Office-filer.		

Aktivera skyddsfunktioner i Windows Exploit Guard

Hur effektiv är åtgärden?	Beskrivning	Potentiell användarpåverkan	Resursåtgång
Mycket effektiv	Använd Windows Exploit Guard med följande delfunktioner (kräver Windows Defender): • Attack Surface Reduction • Exploit Mitigation • Controlled Folder Access Tillämpa en konfiguration som: • Blockerar körbart innehåll från e-postklienten och webbmail. • Blockerar MS Office-applikationer från att starta underprocesser. • Blockerar Office-applikationer från att skapa körbart innehåll.	Låg	Låg

Filtrera e-postinnehåll

Hur effektiv är åtgärden?	Beskrivning	Potentiell användarpåverkan	Resursåtgång
Effektiv	• Säkerställ att inkommande e-post skannas av en anti-virusprodukt innan e-postmeddelandena släpps vidare till användarna eller kan laddas ner via webbläsare. • Analysera ryktet på inkommande filer och webblänkar innan e-postmeddelandet skickas vidare till användarna. • Blockera eller sätt i karantän arkivfiler (t ex zip och RAR) som inte går att inspektera, som till exempel filer som är skyddade med lösenord. • Tillåt att endast godkända filtyper kan komma in som bilagor i e-post (inklusive arkivfiler t ex zip-filer).	Medel	Medel

Filtrera surftrafik

Hur effektiv är åtgärden?	Beskrivning	Potentiell användarpåverkan	Resursåtgång
Effektiv	Använd en funktion som endast tillåter webbsidor med ett känt bra rykte. Blockera åtkomst till domäner och IP-adresser som är ”känt dåliga”. Till exempel sajter som används för phishing, spridning av skadlig kod, styrning av skadlig kod (C2). Blockera exekverbart innehåll generellt och ha en process som tillåter enskilda medarbetare åtkomst av verksamhetsskäl. Blockera okategoriserade URL:er. Filtreringen kan göras i infrastrukturen och/eller webbläsaren.	Medel	Medel

Tillåt inte klientdatorer eller servrar att ansluta direkt till Internet

Hur effektiv är åtgärden?	Beskrivning	Potentiell användarpåverkan	Resursåtgång
Effektiv	Tillåt inte klienter och servrar att ställa direkta DNS-förfrågningar mot resurser på Internet. Använd en e-postgateway och en webbproxy mot Internet. Webbproxyn bör ha förmågan att dekryptera och inspektera HTTPS-trafik. Servrar bör ha en mycket begränsad, helst ingen alls, åtkomst till webbsajter. Servrar bör heller inte ha åtkomst till e-post från externa källor. Servrar bör endast tillåtas kommunicera mot fördefinierade tjänster på Internet. Till exempel uppdateringsservrar.	Medel	Hög

ÅTGÄRDER SOM BEGRÄNSAR KONSEKVENSERNA AV ETT INTRÅNG

Begränsa vilka applikationer som får kommunicera ut mot Internet

Hur effektiv är åtgärden?	Beskrivning	Potentiell användarpåverkan	Resursåtgång
Mycket effektiv	Begränsa i operativsystemens brandväggsfunktion vad som tillåts kommunicera ut mot webbproxy eller motsvarande gateway.	Låg	Medel

Var restriktiv med användningen av administratörskonton

Hur effektiv är åtgärden?	Beskrivning	Potentiell användarpåverkan	Resursåtgång
Mycket effektiv	Tillåt endast nödvändiga roller inom IT-organisationen att kunna logga in på en server eller klienter med lokala administratörsrättigheter. Använd inte administratörskonton för att läsa e-post eller vid webbsurf. Ett administratörskonto som är giltigt på servrar ska inte vara giltigt på klienter och vice versa.	Medel	Hög

Installera säkerhetsuppdateringar för operativsystem

Hur effektiv är åtgärden?	Beskrivning	Potentiell användarpåverkan	Resursåtgång
Mycket effektiv	Installera säkerhetsuppdateringar för operativsystem så fort som möjligt. Kritiska sårbarheter som bedöms utgöra en hög säkerhetsrisk bör ”patchas” inom 5 arbetsdagar. Använd inte operativsystem som inte längre stöds av leverantören.	Låg	Medel

Använd stark autentisering vid inloggning i klientdatorer och servrar

Hur effektiv är åtgärden?	Beskrivning	Potentiell användarpåverkan	Resursåtgång
Mycket effektiv	Använd stark autentisering, så kallad flerfaktorsatutentise-ring, vid inloggning i klientdatorer och servrar. Använd även stark autentisering för VPN, RDP, SSH och andra tjänster som är nåbara via fjärrinloggning.	Medel	Hög

Avaktivera lokala administratörskonton

Hur effektiv är åtgärden?	Beskrivning	Potentiell användarpåverkan	Resursåtgång
Mycket effektiv	Stäng av lokala administratörskonton alternativt ha slumpartade och unika lösenord för dessa konton som användarna inte känner till. Microsoft LAPS är ett verktyg som periodiskt kan ändra lösenordet för det lokala administratörskontot på varje dator i Windows-domänen till ett slumpgenererat lösenord.	Låg	Låg

Skydda inloggningsuppgifter

Hur effektiv är åtgärden?	Beskrivning	Potentiell användarpåverkan	Resursåtgång
Mycket effektiv	Använd Microsoft Credential Guard eller motsvarande för andra operativsystem för att skydda inloggningsuppgifter.	Låg	Låg

Segmentera nätverket

Hur effektiv är åtgärden?	Beskrivning	Potentiell användarpåverkan	Resursåtgång
Effektiv	Var ytterst restriktiv med att tillåta kommunikation från en Internetexponerad server på ett DMZ-nätverk in till det interna nätverket. Tillåt inte direkt kommunikation mellan klienter. All kommunikation bör gå igenom en filtrerande funktion. Detta kan exempelvis begränsas i operativsystemets brandvägg. System- och nätverksadministration bör ske från dedikerade nätverkssegment som inte har åtkomst till Internet. Utvecklings- och testverksamhet bör använda nätverkssegment som är separerade från produktionsmiljön.	Låg	Hög

Använd dedikerade klienter eller terminalservrar för administration av infrastruktur

Hur effektiv är åtgärden?	Beskrivning	Potentiell användarpåverkan	Resursåtgång
Effektiv	Använd dedikerade klienter eller terminalservrar utan åtkomst till e-post och webbsurf för administration av infrastruktur. Även här bör man vara restriktiv med användning av lokala administrationsrättigheter.	Medel	Medel

ÅTGÄRDER FÖR ATT I TID UPPTÄCKA OCH HANTERA INTRÅNG

Daglig säkerhetskopiering

Hur effektiv är åtgärden?	Beskrivning	Potentiell användarpåverkan	Resursåtgång
Mycket effektiv	För att mitigera skadeverkningar från ransomware är daglig säkerhetskopiering av viktig verksamhetsinformation, mjukvara och konfigurationer/inställningar i infrastrukturen viktig. Detta bör lagras off-line med en lagringstid på minst tre månader. Testa återställning minst en gång per år eller vid väsentliga förändringar i infrastrukturen.	Låg	Hög

Kontinuerlig säkerhetsövervakning och incidenthantering

Hur effektiv är åtgärden?	Beskrivning	Potentiell användarpåverkan	Resursåtgång
Mycket effektiv	Detektionsförmåga, d v s förmågan att upptäcka it-angrepp kräver specialistkompetenser, centraliserad insamling av operativsystemsnära loggdata i kombination med data från nätverkssensorer samt rutiner. Det här är en mycket effektiv it-säkerhetsåtgärd och verksamhet för att komplettera alla förebyggande åtgärder men vi är medvetna om att det inte är alla organisationer som har de nödvändiga resurserna. För organisationer med otillräckliga resurser gäller det att hitta ett sätt att avsätta tillräckliga resurser för att visualisera avvikelser och söka efter avvikelser åtminstone ett par gånger i veckan. Alternativt köpa säkerhetsövervakning som tjänst. Exempel på händelser som bör kunna upptäckas: • Microsoft Office-applikation, PDF-läsare eller webbläsare startar avvikande aktivitet i klient eller server. • Filer som exekverar från kataloger där organisationens mjukvara normalt inte kör ifrån. • En klient eller server inleder kommunikation med externa IP-adresser eller frågar efter DNS-namn som är avvikande. • Klient kommunicerar med en annan klient. • Larm från anti-virusprodukt. • Powershell i Windows försöker kommunicera på nätverket eller användare utanför it-avdelningen använder Powershell. • En klient laddar ner ovanligt stora mängder data från domänkontrollant.	Låg	Hög

Installera en agentbaserad loggningsfunktion på klientdatorer som är exponerade mot Internet

Hur effektiv är åtgärden?	Beskrivning	Potentiell användarpåverkan	Resursåtgång
Mycket effektiv	Installera en mjukvara som samlar in loggdata från operativsystemet, så kallad Endpoint Detection and Response-verktyg (EDR). Den typen av verktyg kan logga och skicka loggdatat till ett centralt system för logghantering, larmregler samt såväl automatisk som manuell logganalys (Threat Hunting). Kommersiella EDR-verktyg kan även ha funktionalitet för att vidta motåtgärder vid vissa typer av beteenden. Microsofts Sysmon kostar inget och är lämplig som ett insteg för ändamålet att öka visibiliteten i era klienter och servrar.	Låg	Hög

Använd centrala funktioner för logginsamling, lagring, sökning samt visualisering

Hur effektiv är åtgärden?	Beskrivning	Potentiell användarpåverkan	Resursåtgång
Effektiv	En centraliserad logghanteringsplattform kan användas för att se vilka säkerhetshändelser som inträffar i hela miljön och är en förutsättning för att ha egen detektions- och incidenthanteringsförmåga. Den här funktionaliteten kan tillhandahållas av så kallade SIEM-produkter eller andra typer av produkter som gör det möjligt att visualisera och söka i stora mängder data.	Låg	Hög