NATIONELLT CYBERSÄKERHETSCENTER

Åtgärder för ett säkrare digitalt privatliv

Rekommendationer för ledande befattningshavare, nyckelpersoner och experter

Nationellt cybersäkerhetscenter (NCSC)

www.ncsc.se

ncsc@ncsc.se

NATIONELLT CYBERSÄKERHETSCENTER

Åtgärder för ett säkrare digitalt privatliv

Är ditt privata digitala liv en språngbräda för hotaktörer som vill påverka din organisation? När organisationens säkerhetsarbete uppnått en grundnivå letar hotakörer inom cyberområdet efter nya angreppssätt – ett sådant sätt kan vara ditt digitala privatliv, som blir en väg in till organisationens information.

Rekommendationerna nedan riktar sig till dig som arbetar i svensk offentlig sektor eller i näringslivet. Även om du redan själv vidtagit grundläggande åtgärder, är det alltid viktigt att följa din säkerhetsorganisations råd och rekommendationer. Är du en ledande befattningshavare, nyckelperson eller expert, rekommenderar myndigheterna i NCSC att du snarast inför säkerhetsåtgärderna beskrivna här, både för att skydda ditt digitala privatliv och din organisation. Använd din arbetsgivares digitala tjänster, enheter och appar för att utföra arbetsuppgifter och utbyta arbetsrelaterad information. Där finns avvägda skyddsåtgärder införda för att säkerställa att informationen i din organisation har rätt skydd. Hotaktörer kan bland annat vara intresserade av att nå skyddsvärd information eller att hålla information och it-system gisslan för att utkräva en lösensumma - ofta kallat ransomware, gisslanprogram eller utpressningsvirus.

Många organisationer arbetar systematiskt med sitt informations- och it-säkerhets-arbete, vilket kan ge en god grundnivå av skydd. Men hotaktörerna utvecklar ständigt sina förmågor för att angripa områden där skyddet inte är lika starkt. Utan rätt införda skyddsåtgärder, även för ditt digitala privatliv, kan hotaktörer använda dig som en språngbräda för att nå din organisation eller för att försöka påverka dig i något syfte.

Exempel på hotaktörers tillvägagångssätt

I december 2023 varnade den amerikanska cybersäkerhetsmyndigheten CISA tillsammans med ett antal andra nationella säkerhetstjänster för hur en statlig hotaktör på ett antal olika sätt angripit organisationer inom akademin, försvarssektorn, myndigheter, offentlig sektor, tankesmedjor och politiker. Bland annat har angreppen skett i USA, Storbritannien och ett antal andra Nato-länder. Angreppen har framför allt riktats mot ledande befattningshavare, nyckelpersoner och experters digitala privatliv, men även mot organisationens it-miljö. Angreppen har bland annat skett genom:

- Falska identiteter i sociala media och e-postkonton. Dessa har samma namn som personer i den privata eller professionella kontaktkretsen för att uppfattas som legitima konversationer.
- Falska domäner vilka liknar legitima domäner som användaren har regelbunden kontakt med. Detta för att uppfattas som legitima e-postkonversationer.
- Falska inloggningssidor skapade av hotaktören, där den drabbade lurats att logga in till exempelvis en samarbets- och/eller fildelningsplattform för att nå information. Istället stjäls den drabbades inloggningsuppgifter och/eller inloggningsbiljetter (”session cookies”).
- Initiala konversationer genom sociala media och/eller e-post kring verkliga och legitima ämnen, vilka i senare skeden lett till länkar innehållande skadlig kod eller falska inloggningssidor. Länkarna har bland annat använt välkända och legitima samarbets- och fildelningsplattformar som missbrukats av hotaktören i angreppen.

1: Uppdatera

Alla enheter, program och appar kan innehålla fel och svagheter, vilka kan utnyttjas av hotaktörer för att på olika sätt angripa dig och din information. Använd därför enheter, program och appar som underhålls av tillverkaren och som har en historik av regelbundna uppdateringar. Genom att uppdatera din enhet så snart en uppdatering blir tillgänglig skyddar du den och din information. Både operativsystemet och applikationer behöver uppdateras, en del uppdateringar kräver en omstart för att få genomslag. Finns funktioner för automatiska uppdateringar, använd dessa. Program och appar som inte underhålls och uppdateras innebär säkerhetsrisker och bör därför bytas till ett annat alternativ. Även enheter som inte uppdateras behöver bytas ut till nya, vars operativsystem och programvara regelbundet underhålls av tillverkaren.

Glöm inte bort att hålla dig själv uppdaterad om nyheter och säkerhetsupp-dateringar som kan vara viktiga för ditt digitala privatliv. Till exempel rörande säkerhetsinställningar i datorer, smarta och uppkopplade enheter samt appar.

2: Säker identifiering och lösenordshantering

Bra lösenord kan vara svåra att skapa och att komma ihåg, men de är viktiga för att skydda ditt digitala privatliv mot intrång. Hotaktörer använder ofta lösenord som är enkla att gissa eller lösenord från tjänster som hackats för att prova om användare har återanvänt samma lösenord för flera tjänster. Det är extra viktigt att inloggningen till din privata e-post är säkrad, den är ofta ”huvudnyckeln” till ditt digitala privatliv. En hotaktör kan annars använda ditt e-postkonto för att återställa lösenord för dina andra digitala tjänster.

Genom inloggningsmetoder där du kombinerar en fysisk enhet med en kod stärks din identifiering. Det kan t.ex. göras genom att logga in med en identifieringsapp (authenticator app) på din smartphone eller med säkerhetsnyckel som du ansluter till din enhet tillsammans med en pinkod, ofta beskrivet som tvåfaktorsidentifiering (multi- eller two-factor authentication). Dessa typer av identifiering är att föredra framför identifiering som baseras på sms-meddelande. Där du måste använda lösenord, välj långa fraser – de är enklare att komma ihåg än kortare, är komplexa och samtidigt svårare för hotaktörer att knäcka. Ett bra stöd för att förenkla hanteringen av lösenord kan vara en lösenordshanteringsapp (password manager), vilken kan skapa och spara ett långt och komplext lösenord per digital tjänst du använder.

3: Säkerhetskopiera

Skapa säkerhetskopior av information som är viktig för dig, så att du kan återskapa den om du drabbas av skadlig kod, ett fysiskt haveri eller stöld av en enhet. Allra bäst är om säkerhetskopieringen kan ske ofta och med automatik, så du inte behöver vidta regelbundna manuella åtgärder. Även om du använder en tjänst för att lagra din privata information är det bra att ha en egen kopia tillgänglig på en annan enhet, helst en som du kan förvara på en säker plats. Om olyckan skulle vara framme hos din tjänsteleverantör och informationen inte längre är tillgänglig genom tjänsten, kan du då ändå få tilltillgång till din information. Säkerställ även att du kan använda säker identifiering (beskrivet ovan) för en tjänst, om du väljer att använda en sådan.

4: Bilagor och länkar

Olika former av nätfiske (phishing) är en mycket vanlig metod för att lura en användare att använda en falsk inloggningssida, där användarens inloggningsuppgifter stjäls. Var försiktig med att öppna bilagor och att klicka på länkar som skickas till dig i e-post, meddelanden och genom sociala media. Bifogade filer och länkar kan innehålla skadlig kod som smittar din enhet och som låser eller raderar din information. Om någon ber dig logga in genom en bifogad länk bör du vara extra försiktig. Måste du logga in till en tjänst för att nå information som beskrivs i ett mejl, logga istället in till tjänsten genom att själv ange dess adress i en webbläsare istället för att klicka på en bifogad länk. Använd i första hand enkla textformat för att utbyta information med andra, avancerade filformat kan innehålla skadlig kod.

5: Surfa inte oskyddat

Använd och aktivera den inbyggda säkerhet som finns i din enhet, så som t.ex. anti-virus- och brandväggsfunktioner. Saknar din enhet säkerhetsfunktioner, sök professionellt stöd för en rekommendation om en lösning att använda för dina behov. Minimera din användning av öppna publika wifi-nätverk, då dessa enkelt kan avlyssnas eller påverkas av hotaktörer. Acceptera aldrig varningar om certifikatfel, även om instruktionerna för den uppkoppling du vill nyttja säger det. Anslut i stället till internet genom betrodda anslutningar, till exempel genom din anslutning hemma eller genom din mobiloperatörs nätverk, se även rekommendationerna nedan om Smarta enheter i hemmet. Använd främst webbsidor med krypterad anslutning, i din webbläsare kan du se att anslutningen är krypterad genom https:// i adressfältet. Det är särskilt viktigt att anslutningen är krypterad när du anger ditt namn och lösenord för att logga in på en webbsida, ditt användarnamn och lösenord kan annars enkelt avlyssnas.

6: Skydda din enhet

Var försiktig med din enhet, överväg att aktivera inbyggda funktioner för utökad säkerhet, t.ex. låst läge (Lockdown Mode) om du använder iPhone. Om du lämnar den obevakad kan någon stjäla eller manipulera den, lämna därför inte enheten obevakad och/eller upplåst. Dela inte med dig av din pinkod eller ditt lösenord för att logga in till din enhet. Hotaktörer kan påverka och förstöra din enhet om du ansluter okända enheter till den. Ladda därför din enhet med en betrodd laddare och sladd, använd inte publika usb-uttag. Var försiktig med att använda enheter du fått från andra, t.ex. usb-minnen och ta för vana att formatera nya usb-minnen innan du använder dem. Utvärdera

tillsammans med din säkerhetsorganisation om du behöver en separat mobil enhet för arbetet, skild från ditt digitala privatliv.

7: Sociala media

Sociala media kan användas av hotaktörer för att kartlägga dig, din familj, dina vänner och ditt rörelsemönster. Använd därför de funktioner som finns i sociala media-plattformar för att begränsa den information du delar med dig av och med vem informationen delas. Var också försiktig med vem du kommunicerar med genom sociala medier. Olika meddelande-appar och sociala medier är också en kanal som nyttjas av hotaktörer för att kringgå traditionella skydd för att stoppa phishing och skadliga bilagor. Var därför extra uppmärksam och försiktig med länkar och bilagor som sänds till dig genom meddelande-appar och sociala medier (se ovan).

8: Skydda din kommunikation

I digitala kommunikationstjänster finns i stort sett alltid tjänster och system som agerar mellanhänder för att vidarebefordra din kommunikation. Dessa mellanhänder kan kartlägga, ändra och avlyssna din kommunikation i olika syften. Var därför försiktig med att utbyta känslig och privat information genom exempelvis sociala medier, e-post och mobila textmeddelanden, eftersom informationen genom dessa verktyg saknar skydd för konfidentialitet, riktighet och integritet. Skydda din privata kommunikation så som meddelanden och samtal genom totalsträckskrypterade funktioner (end-to-end krypterade funktioner). Genom att använda totalsträckskrypterade tjänster kan bara sändare och mottagare av kommunikation kan ta del av informationen, även när informationen överförs genom internetbaserade kommunikationstjänster.

9: Smarta enheter i hemmet

Smarta enheter i hemmet kan nyttjas av hotaktörer för att på olika sätt ta del av vad som sker i ditt hem. Var därför försiktig med var och hur du ansluter enheter som smarta assistenter, högtalare och andra hjälpmedel med mikrofoner och kameror i ditt hem. Enheterna är var för sig små datorer som behöver underhållas och uppdateras på samma sätt som beskrivits ovan. Det är också viktigt att byta enheternas standardlösenord de levererats med till ditt eget, samt om möjligt använda säker identifiering med två faktorer (beskrivet ovan) om enheten ansluter till någon typ av molntjänst. Använder du smarta enheter i ditt hem och arbetar hemifrån kan du behöva flytta dem från den plats i hemmet du arbetar. Kontakta din säkerhetsorganisation för råd och stöd gällande säkra uppkopplingar vid distansarbete.

Mer information

Kontakt och mer information

Kontakta Nationellt cybersäkerhetscenter: ncsc@ncsc.se

Mer tips och råd kring hur du säkrar ditt digitala privatliv

https://www.internetstiftelsen.se

https://www.ssfcybersakerhet.se

https://www.ncsc.gov.uk

https://www.cyber.gov.au