Grundläggande Cybersäkerhet

Oktober 2020

SRS har under ECSM, **European Cybersecurity Month**, publicerat praktiska råd och tips för att bidra till att höja medvetenheten kring cybersäkerhet. Våra cybersäkerhetstips har fokuserat på åtgärder som kan göras inom områdena människor, processer och teknik. Nedan finner ni våra tips sammanfattade under

- Lösenord
- Uppkopplade enheter
- Appar, program och övriga tjänster

Lösenord

Ditt lösenord är en virtuell nyckel som förhindrar obehörig access till dina konton och skall behandlas som en värdehandling.

Skapa säkra lösenord. De 15 miljarder vanligaste lösenorden finns läckta och till salu billigt på nätet. Använder du något av dessa försämrar det kraftigt dina kontons säkerhet. För att undvika detta – skapa alltid unika och separata lösenord för varje system och webbplats. Se punkten nedan.

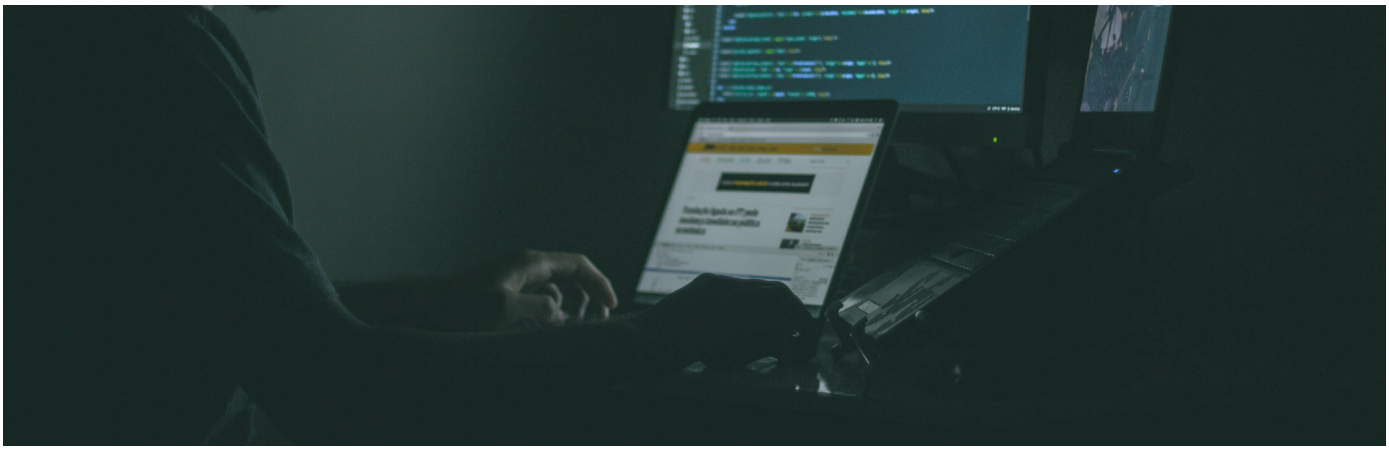
Använd lösenordsordshanterare. SRS rekommenderar tex. F-Secure Key för att generera starka och unika lösenord på minst 15 tecken. En bättre speldator kan göra 40 miljarder försök i sekunden på ett lösenord, ett lösen om 9 tecken tar då ca 6 mån att knäcka medan 7 tecken endast tar 28 min. Om ditt lösen finns med på en lista, en läcka eller t.ex i en ordbok, så kommer det ta 0,1 sekunder för ordet att bli knäckt. Längd och icke förutsägbarheten har betydelse.

Som organisation:

- Ha ett regelverk för vilka lösen som kan och bör sättas
- Testa regelbundet att lösen inom organisationen håller måttet

SRS Security, PO Box 244, SE-101 24, Stockholm
+46 8 440 90 70 | mail@srsgroup.se | www.srsgroup.se

Aktivera multifaktorautentisering för alla onlinetjänster. Idag är det enklaste sättet att försvåra phising-bedrägeri två-faktorautentisering eller multifaktorautentisering (MFA) som det också kallas. Kortfattat innebär det att du ökar säkerheten genom att använda två olika verifieringssteg och vår rekommendation är att använda en app och inte SMS då SMS lätt kan hackas och numret styras om till annat SIM-kort.



Uppkopplade enheter

Följande skall iakttas för alla uppkopplade enheter som datorer, telefoner, trådlösa enheter, klockor, osv.

Se till att göra offline-backuper. Utpressningsvirus är en skadlig kod som krypterar filer och kräver en summa i utbyte mot dess återställning. Anledningen till att backuperna behöver vara offline är att utpressningsvirus inte bara tar dina lokala filer utan letar sig runt i nätverket och krypterar allt den kommer åt, dvs hela IT infrastrukturen inklusive de backuper som finns internt på ditt nätverk. Skilda nätverksdelar och behörigheter hjälper att minimera spridning. SRS rekommenderar att göra regelbundna backuper till externa krypterade offline hårddiskar.

Som organisation:

- Tillse ett regelverk för hur och med vilken frekvens backuper ska tas samt testa att återställa från backup för att säkerställa att det är genomförbart

Koppla inte upp enheter på nätverk utan godkännande. Om en enhet (tangentbord, kaffemaskin, server etc.) kopplas in på nätet utan att uppfylla interna säkerhetskrav är risken att enheten blir en dörr in till nätverket. Väl inkopplad på strategisk plats riskerar hela nätverket att bli avlyssnat och övertaget. Var vaksam och ifrågasätt oväntade manicker i konferensrum och kontorsmiljö.

Som organisation:

- Inför autentisering på MAC adresser för att förhindra obehörig access
- Bevaka kontinuerligt nätverk efter okända enheter
- Implementera en process för hur enheter kontrolleras och tillåts

Anslut dig bara till trådlösa nätverk du litar på eller använd VPN. VPN hjälper till att skydda din integritet på nätet genom att kryptera din trafik. Hackare använder sig av gemensamma internetuppkopplingar och WIFI-nätverk som dörr in till din dator. Om du ansluter dig till ett Wi-Fi nätverk på ett café eller ett flygplan kan en angripare enkelt se adresser till de webbsidor du besöker samt data från dina mobiltelefonapplikationer. Genom att använda ett säkert VPN kommer din trafik att krypteras och angripare har då inte längre tillgång till dina filer. Välj betal VPN-tjänster från en leverantör och ett land som du litar på. VPN leverantörer kan se delar av din icke krypterade trafik och gratis VPN-tjänster säljer sannolikt din data för att finansiera tjänsten.

Som organisation:

- Förse dina anställda med en VPN-lösning på arbetsdatorerna

Koppla aldrig in en extern enhet från någon du inte litar på i din dator. Skadliga USB-minnen är ett effektivt sätt för angripare att ta sig in i en dator och snabbt infektera den med virus. I värsta fall kan USB-enheter fysiskt förstöra en dator genom att ladda upp kondensatorn som sedan ger datorn en kraftig strömstöt och förstör den. Var försiktig när någon ber om hjälp att skriv ut dokument från en USB eller att få ladda sin telefon i din dator.

Som organisation:

- Informera medarbetare om farorna med externa enheter så att alla är extra varsamma

Försvåra avlyssning genom att vara extra uppmärksam och använda svåra lösenord. Avlyssning kan gå till på många olika sätt, antingen genom fysisk närvaro eller genom tekniska lösningar. Kameror och mikrofoner kan göras oerhört små och enkelt byggas in i sladdar och enheter som kamoufleras till vanlig IT-utrustning. För att få ut informationen utnyttjas ofta sårbara nätverk med dåliga lösenord. Detta är en enkel väg att gå då inkräktaren inte behöver sätt upp en egen väg för överföring av data ut på Internet.

Som organisation:

- Kontrollera regelbundet konferensrum efter kablar och enheter som ej ska finnas där

Stäng av (inte bara avaktivera) platstjänster, WiFi och Bluetooth när de inte används. Det är inte ovanligt att appar och program gång på gång ber om access till din plats, dina foton osv. Det räcker ofta med att du bara en gång klickat på ”ja” och sedan är det på för alltid, även när du inte vill det. I samband med lansering av nya versioner kan det komma funktioner som automatiskt slår på saker du inte vill. SRS rekommenderar att utgå från att allt ska vara avstängt och slå på saker i efterhand när de behövs samt att kontrollera inställningar och nya funktioner efter varje större uppdatering.

Skilj på yrkesliv och privatliv. Särskilj dina privata och yrkesmässiga enheter samt enheter med skyddsvärd information på. Installera inte appar för privat bruk på verksamhetens utrustning och återanvänd inte digitala tillgångar från verksamheten som mailadresser och lösen.

Som organisation:

- Utforma policy och styrdokument och utbilda de anställda för att få en självgående säkerhetskultur

Appar, program och övriga tjänster

Följande skall iakttas för alla appar, program och övriga tjänster

Var inte inloggad som administratör. Genom att inte vara inloggad som administratör minskar du de tekniska sårbarheterna med 80-95%. Ett konto med administrationsrättigheter har tillgång till hela datorns vitala operativsystem och filer samt har behörighet att göra ändringar i system. SRS rekommenderar att ha ett separat konto för admin och endast använda det då det är nödvändigt.

Som organisation:

- Ha särskilda konton och enheter för system- och behörighetsadministration
- Utför regelbundet hot- och riskbedömningar inkl. utvärdering av skyddsvärda tillgångar

Stäng av alla makron. Makron används för att automatisera olika funktioner för att underlätta för användare att utföra vissa uppgifter eller för att visa olika typer av innehåll. Kortfattat kan man säga att ett makro är en serie kommandon som spelas in så det kan spelas upp vid ett senare tillfälle. En angripare kan skriva ett makro som kan göra i stort sett samma saker som annan skadlig kod, exempelvis stjäla data, kryptera dina filer, skicka e-post till alla dina kontakter, bara genom att du öppnar ett dokument i Word, Excel eller Powerpoint. Stäng därför av alla makron och tillåt bara makron i dokument som finns på betrodda nätverksplatser.

Som organisation:

- Tillåt inte att användarna aktiverar makron själva

Vänta inte med uppdateringar. I snitt tar det drygt en månad ifrån utkommen uppdatering till att cyberattacker börjar genomföras, dock sker 25% av attackerna redan inom en vecka. Se därför till att uppdatera dina system snarast möjligt, helst inom 48 timmar.

Som organisation:

- Lista skyddsvärda tillgångar för att avgöra vilka som är de mest kritiska
- Bevaka de system ni använder för akut uppkomna sårbarheter/uppdateringar

Brandväggen ska var på, även för utgående trafik. En brandvägg är ett säkerhetsverktyg som filtrerar inkommande och utgående trafik från din enhet och internet. Den hindrar även informationsläckor vid interna felkonfigureringar samt att skadlig kod installeras och sprids. Många förstår vikten av att ha en brandvägg som skyddar mot inkommande trafik men missar att blockera tjänster rörande utgående trafik.

Som organisation:

- Stäng av in och utgående trafik för protokollen nedan och tillåt endast trafik från betrodda nät
    - SMB och TFTP /FTP
    - MS RPC och SNMP
    - SMTP och IRC
    - DNS och ICMP
- Konfigurera brandvägg att larma om någon intern enhet försöker använda TFTP eller IRC då det kan indikera att det finns skadlig kod på nätverket

Skriv inget i ett mejl som du inte hade skrivit i ett vykort. När ett e-postmeddelande rör sig över Internet kan det likt ett vykort läsas på vägen. Mellan avsändare och mottagare finns det ett antal mailservrar och proxyservrar som meddelandet rör sig emellan och väl framme vid destinationsservern kan en möjlig smygläsare vara e-postadmin. Använd krypterade kommunikationskanaler för känsligt informationsutbyte alternativt lägg viktig information i ett dokument som du krypterar innan sändning. Använd epostkryptering som exempelvis SMIME eller PGP.

Granska de molntjänster ni använder. Idag går många över till att använda molntjänster men missar både att ställa säkerhetskrav på leverantören och att göra en ordentlig riskanalys för att säkerställa rätt lämpliga säkerhetsåtgärder. SRS rekommenderar att kolla upp vem leverantören och dess ägare är; vilka lagar och regler gäller för dem? Hur ser affärsmodellen ut? Om tjänsten är gratis eller väldigt billigt finns det risk för att det är ”ni som är produkten”. Undersök även vad leverantörens definition av säkert är; vilka standarder arbetar de efter? Vilka certifieringar och kontroller har de genomgått?

Som organisation - se över:

- Kontext: Vem är du och din organisation, vilka lagar och regler gäller för er, vilken riskaptit har ni?
- Skyddsvärden: Vilken Information vill du skydda (personal, anseende, tillgänglighet mm)?
- Aktörer: Vilka vill du skydda er mot och vad har de för förmågor?

Skydda din information genom att kryptera dem. Kryptering är ett effektivt sätt att skydda digital information, antingen i vila lokalt på din eller din leverantörs enhet eller i rörelse. Information i rörelse innebär information under transport, förflyttning över ett nätverk från en enhet till en annan, så som e-post, chat eller webbsurf. När information skyddas är det viktigt att ta hänsyn till båda dessa tillstånd. Exempelvis kan administratören av en e-postserver eller spamfilter i regel alltid gå in och läsa mejl eftersom kryptering bara sker mellan e-postservrar och mellan servern och din enhet. SRS rekommenderar att kryptera hårddiskar och USB-stickor samt att använda krypterade kommunikationskanaler. Lösenordskydda känsliga dokument som skickas över kanaler som inte har ”end-to-end-encryption (E2EE)”.

Var försiktig med vilka avtal du godkänner. Det finns många appar som är både tilltalande och roliga men tyvärr kan dessa innehålla väldigt tveksamma avtal som de flesta av oss bara klickar förbi genom att trycka på ”Godkänn”. Avtalen kan bestå av vilken data som kommer att samlas in, vad leverantör får tillgång till och vilka som får ta del av informationen. I många fall ändras avtalen under tidens gång. Läs eller kontrollera app-/tjänsteavtal och informationsinhämtning med någon som är kunnig på området. Räkna med att lösen och information som behandlas av appen-/tjänsten kommer bli tillgänglig för många fler än du tänkt dig.

Basera inte säkerhet på personuppgifter. Framför allt i Sveriges öppna samhälle kan man få tag på det mesta. Att basera säkerhetsfrågor på personuppgifter som exempelvis ”Vad är din mors födelsenamn?” gör det enkelt för kriminella aktörerna att ta reda på svaret på vissa frågor. Detta beror också på att vi delar med oss om så mycket om oss själva på nätet och sociala medier. Med dagens högupplösta kameror är det extra viktigt att tänka på vad som publiceras, det går att kopiera fingeravtryck och lura viss ansiktsigenkänning med dessa bilder. SRS rekommenderar att kontrollera och begränsa vad, när och till vilka som du postar och visar saker för.

Var observant på vilka som försöker nå ut till dig över sms, telefon och mail. Ett simpelt muntligt svar som ”Ja” skulle kunna leda till att någon annan köpt sig en bil med dina pengar genom ditt medgivande. Bedragare klipper ihop en röstinspelning så att det låter som att tex du köpt en bil av dem. Phishing, smishing, vishing, whaling, alla ingår i konceptet ”social engineering” som innebär att hotaktören försöker lura fram känslig information från sitt offer eller få hen att trycka på en länk som i sin tur kan leda till att en enhet blir övertagen. Dessa metoder är idag betydligt mer förfinade än för bara något år sedan.

Som organisation:

- Håll kontinuerliga säkerhetstester och utbildningar för era anställda

Utbilda varandra, 80% av alla attacker börjar med ett mejl. Ransomware, kryptovirus, utpressningsprogram är en typ av skadlig programvara vars syfte är att utpressa genom att hindra användare från att komma åt sina system eller personliga filer. För att återfå tillgång krävs lösenbetalning. Cyberkriminella är nästan alltid bara ute efter pengar och genom att blockera din information och tjänster eller hota med att läcka det så har de en direkt källa till inkomst – dig. SRS rekommenderar att spärra körning av macron och använd nyare office-format.

Konfigurera SPF för att förhindra förfalskade domännamn. Det finns gratis mailservar att köra på sin dator där man kan ange vem avsändaren ska vara, dvs att alla kan skicka mejl och uppge sig vara @regeringen.se eller @whitehouse.gov. För att se att det är rätt avsändare måste mottagaren ställa in att kontroll ska göras på vilka servrar och datorer som får skicka e-post till dig. Detta kallas för Sender Policy Framework (SPF) och är en metod för att förhindra att e-post skickas med förfalskade domännamn i avsändaradresser. Tänk på att outlook sällan skriver adressen inom organisationen utan bara visningsnamn samt att mobiler bara visar visningsnamn för alla mejl men genom att påbörja ett svar eller klicka på namnet så ser man hela adressen.

Har du funderingar kring din cybersäkerhet?

Kontakta oss på cybersecurity@srsgroup.se så leder vi dig rätt!

SRS Security, PO Box 244, SE-101 24, Stockholm
+46 8 440 90 70 | mail@srsgroup.se | www.srsgroup.se

SRS