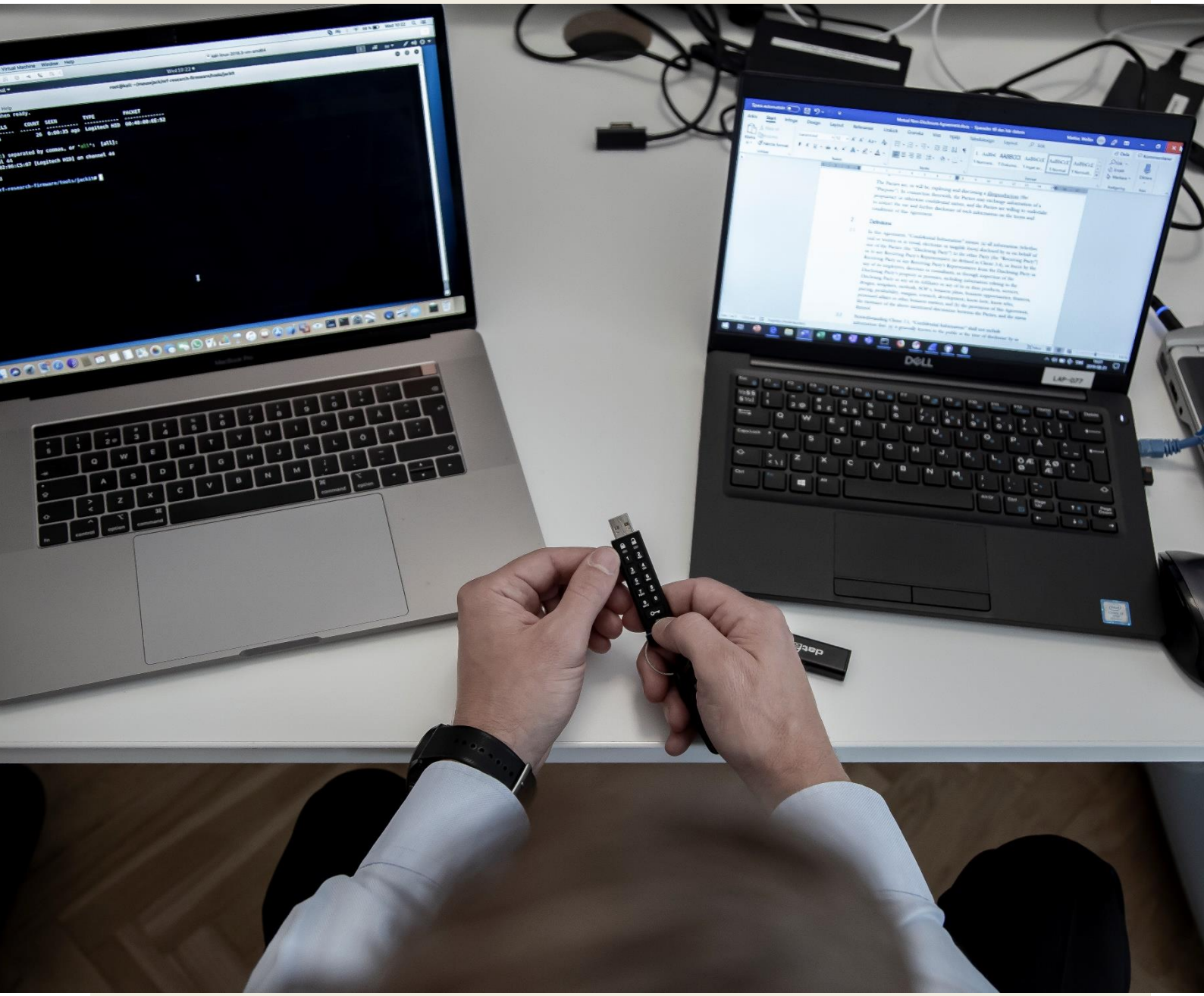
IT-säkerhet och instruktioner

Vid distansarbete från hemmet

2020



Utmaningar vid distansarbete från hemmet

Det pågår en stor omställning inom arbetslivet just nu som en konsekvens av den rådande Covid19-pandemin. Folkhälsomyndigheten bedömer att det pågår en allmän samhällsspridning i Sverige och uppmanar därför fortsatt till allmänheten att vida åtgärder för att begränsa smittspridningen. För att minimera risken för fortsatt spridning förväntas allt fler uppmanas till arbeta hemifrån. **Men vad innebär det när ett antal utan motstycke bestämmer sig för att arbeta på distans samtidigt?** Den sammanställning som följer nedan baseras på CERT.ses lägesbild och SRS kompletterande rekommendationer:

Situationen utnyttjas av kriminella aktörer och samtliga organisationer uppmanas till ökad vaksamhet och medvetenhet gällande IT- och informationssäkerhet, särskilt med tanke på att allt fler medarbetare arbetar hemifrån. **När organisationer gör sig beroende av tekniska lösningar i högre grad är det också viktigt att ha en större förmåga att begränsa onödig riskexponering samt upptäcka och hantera incidenter för att minimera deras konsekvenser.** Vi uppmanar samtliga organisationer att betänka och skapa förutsättningar för att lösa ut följande frågeställningar:

1). Organisationen behöver **adekvat infrastruktur, utrustning och förutsättningar** för att de anställda ska kunna arbeta i hemmet. När det gäller tekniska förutsättningar handlar det ofta om åtkomst till arbetets nätverk på ett säkert sätt, tex. krypterat via VPN-anslutning, gärna med tvåfaktorsautentisering.

2). Flera medarbetare riskerar att **ansluta sig via sina hemmanätverk som inte är säkra.** De flesta bredbandsanslutna hem uppskattas ha över 20 anslutna enheter om man räknar in hushållets telefoner, bärbara datorer, termostater, hemmalarm, kameror, Wi-Fi, TV-apparater, etc. Dessa enheter kan vara sårbara punkter för angrepp eller informationsläckage då majoriteten av dessa enheter är varken säkra eller regelbundet uppdaterade.

3) Fler distansanslutna användare ställer ett **högre krav på organisationens IT-avdelningar** att övervaka nätverkens bandbredd, VPN-funktionalitet och anslutningar så att medarbetarna kan utföra sina arbetsuppgifter. Det innebär också en ökad belastning på organisationernas infrastruktur men också på de olika internetleverantörerna

4) Förutom IT-säkerhet finns risker som behöver övervägas i fråga om informationssäkerhet och vilken möjlighet den som arbetar hemifrån har att **hantera känslig information på ett säkert sätt.**

Det här kan du som arbetsgivare behöva tänka på:

- ❑ Säkerställ att alla medarbetare känner till era rutiner och policyers för distansarbete.
- ❑ Se till att anställda som arbetar hemifrån kan komma åt resurser de behöver för att göra sitt jobb på ett säkert sätt (tex. VPN, tvåfaktorautentisering). I rådande situation kan en acceptans för avvikelser från verksamheten vara högre än den normala säkerhetsstandarden.
- ❑ Se över att IT-supportfunktioner är tillräckligt bemannade, då det kan bli ökad mängd frågor och support gällande anslutning från hemmet. Anställda som inte får hjälp kan lätt ta genvägar som inte är önskvärda utan utgör en säkerhetsrisk för hela organisationen.
- ❑ Tilldela inte slutanvändare administratörsrättigheter. Vanliga användare har sällan behov av att tex. installera programvara på maskinen. Överlåt det till IT-administration att distribuera programvara.
- ❑ Blockera icke-auktoriserad programvara. Tillåt endast att användare kör godkända applikationer.

Det här behöver era anställda tänka på:

- ❑ De största säkerhetsutmaningarna i dag är inte bara tekniska, utan kretsar kring användarbeteenden. Dessa svagheter består främst av en generell okunskap hos den gemene användaren som resulterar i ett sårbart riskbeteende.
- ❑ Medarbetare bör inte använda privat utrustning för arbetsrelaterat arbete om inte det har avtalats och godkänts av din arbetsgivare och ansvarig IT-avdelning. Undvik att använda privata molntjänster såvida de inte klargjorts av arbetsgivaren.
- ❑ Medarbetare bör säkerställ att utrustningen som de ska använda vid distansarbete är väl uppdaterad (såväl maskinvara, operativsystem, tredjepartsapplikationer och antivirussignaturer).
- ❑ All kommunikation med organisationens nätverk och tjänster bör säkras genom att till exempel använda VPN.
- ❑ Medarbetare bör säkerställa att de har tillräcklig internetkapacitet för effektivt distansarbete.
- ❑ Alla användarkonton bör ha starka lösenord och helst med tvåfaktorautentisering.
- ❑ Vid arbete i hemmet ökar risken för att exponera känslig information i större utsträckning än när man arbetar på arbetsplatsen. Medarbetare bör uppmanas till att var extra medveten om vilken typ av information som de hanterar när de jobbar hemmavid och säkerställ att de kan hantera den på ett korrekt sätt även där.
- ❑ För att upprätthålla god kapacitet i sina internetanslutningar under tiden de arbetar bör de uppmanas till att koppla ifrån andra enheter från nätverket som inte behövs för arbetet tex. stream-tjänster.

Rekommendationer:

- ❑ SRS uppmanar till särskild vaksamhet gällande IT-incidenter eller andra misstänkta händelser relaterade till Covid19-pandemin. Det förekommer redan online-bedrägerier, där kriminella aktörer utnyttjar situationen för att skicka bedräglig e-post och sms i syfte att komma över kontouppgifter eller sprida skadlig kod. Rapportera in potentiella fall till ansvarig IT-avdelning, SRS och CERT-SE.
- ❑ Utveckla en välformulerad säkerhetspolicy inom organisationen och komplettera denna med rätt utbildningar för att höja kunskapsnivån hos samtliga medarbetare inom organisationen.

Behöver ni ytterligare stöd och assistans?

SRS erbjuder riktade tjänster inom cybersäkerhet, inklusive kompetenshöjande utbildningar för såväl styrelse- och ledningsgrupper som personal. Med beprövad kompetens och bred expertis inom informations- och cybersäkerhet arbetar vi proaktivt för att höja er säkerhet i det digitala rummet.

Genom att kartlägga era unika skyddsvärden, identifiera hot och sårbarheter samt hjälper er vidta anpassade skyddsåtgärder som minimerar era risker. Våra cybersäkerhetsexperter kan stödja med utredningar, forensik och säker hantering av exempelvis anställningsavslut. Vidare erbjuder vi även tjänster som phishing eller candy drop-test som prövar er personals säkerhetsmedvetenhet.

För mer information, vänligen besök https://srsgroup.se/tjanster/cybersakerhet/
eller kontakta oss för vidare konsultation på cybersecurity@srsgroup.se

Appendix: Starka lösenord

Ditt lösenord är en virtuell nyckel som förhindrar obehörig access till dina konton och skall behandlas som en värdehandling. På samma sätt som du inte skickar kopior på dina fysiska hem- och jobbnycklar till någon bör du inte heller göra detta med dina virtuella nycklar. Men ibland kan det vara svårt att veta hur du ska tänka kring dina lösenord eller hur de hanteras på internet. Nedan följer tips och råd för hur du på ett snabbt och enkelt sätt kan stärka dina lösenord:

- ❑ Återanvänd inte samma lösenord till flera olika filer, tjänster eller konton. Hackare knäcker ofta lösenordet på sämre skyddade system och sparar dem för att sedan använda dem till inloggningsförsök på bättre skyddade system.
- ❑ Skriv inte in eller använd lösenord på system/tjänster där ni eller er IT-avdelning inte kan garantera att det finns en godkänd administratör eller programvara
- ❑ Använd så kallade multifaktorautentiseringsfunktioner i så stor utsträckning som möjligt. Stöd för denna typ av metod återfinns bland nästan samtliga onlinetjänster genom till exempel Microsoft Authenticator eller Googles Authenticator, men det går även att använda särskilda USB-nycklar som försvårar falska inloggningsförsök avsevärt. Om möjligt, undvik koder som skickas ut via SMS då denna metod är mindre säker och manipulerbar.
- ❑ Använd lösenordshanterare. SRS rekommenderar F-Secure Key för att genera starka och unika lösenord. För väsentliga lösenord som du måste komma ihåg rekommenderar vi att du använder ett unikt lösenord per tjänst bestående av minst 15 tecken, kommer ihåg långa fraser (ex. "correct horse battery staple"), men låt lösenordhanteraren hantera övriga, mindre viktiga lösenord.

Kom ihåg: Det finns över 15 miljarder lösenord läckta och till salu billigt på nätet. Använder du något av dessa försämrar det kraftigt dina kontons säkerhet. För att undvika detta skapar du helt unika lösenord för de dokument och tjänster som du använder (se punkt ovan). Kontrollera om dina mejladresser/lösenord har läckts på: https://haveibeenpwned.com/.

Uppkopplade enheter och applikationer/program

Följande skall iakttas för alla uppkopplade enheter (datorer, telefoner, trådlösa enheter och klockor):

- ❑ Använd datorns interna brandvägg och tillåt ingen extern kommunikation till datorn.
- ❑ Använd program och inställningar som tillåter dig att spara och rader enheten om den stjäls.
- ❑ Håll privata respektive yrkesrelaterade enheter, liksom enheter med lagrad skyddsvärd information separerade från varandra. Avstå alltid från att koppla samman dessa.
- ❑ Vid behov, ladda endast ner applikationer och program från kända leverantörer och officiella sidor. Undvik gratis-versioner då de ofta säljer vidare din data eller innehåller skadlig kod i sig.
- ❑ Håll alla system och tjänster uppdaterade, som till exempel BIOS, enskilda applikationer, program och anti-virustjänster. Aktivera gärna automatiska uppdateringar. Notera att även Apple-produkter behöver adekvata antivirusprogram. SRS rekommenderar F-Secure SAFE.
- ❑ Installera en VPN som används när du använder Wi-Fi nätverk för att dölja var du befinner dig samt till stor del dölja din enhet på nätverket från andra enheter. SRS rekommenderar F-Secure Freedome eller Express VPN (som fungerar även i Kina).
  Vid anslutning till andra nätverk, t.ex publika WiFi eller delade nät, måste VPN användas

För ytterligare handfasta råd och utbildningsinsatser inom adekvata IT-säkerhetslösningar och metoder för enskilda användare eller organisationer, kontakta cybersecurity@srsgroup.se för vidare konsultation.

SRS a global risk management company which is certified and approved by international authorities, industry bodies and business partners. SRS headquarter is located in Stockholm with representatives in UK, France, Norway, Somalia and Nigeria, and employs over 150 experts worldwide. While confident with proven and successful operational experience from over 45 countries, our services include, among other features:

Cyber Security | Risk Assessments | Security and Safety Training Solutions | Due Diligence

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

SRS