CYBERATTACKERNA HAR ÖKAT KRAFTIGT UNDER COVID-19*
– HUR SÄKERT JOBBAR NI HEMIFRÅN?

För att minska smittspridningen rekommenderar Folkhälsomyndigheten** företag att låta sina anställda arbeta hemifrån i så stor utsträckning som möjligt. Hur säker är IT-miljön utanför kontoret?

Borttappade filer, cyberattacker och en slutkörd IT-avdelning är några riskfaktorer som drabbar både små och stora företag även till vardags, men i kristider är det lätt att få panik och välja första bästa alternativ. Det leder till hemmasnickrade och kortsiktiga lösningar som många gånger äventyrar IT-säkerheten. Så här hanterar du som vd situationen, ökar säkerheten och optimerar IT-kostnaderna när fler jobbar hemma.

RISKFAKTOR 1:

SLARV OCH SNABBA LÖSNINGAR

Om man inte har ett bra IT-system i grunden finns det en risk att medarbetarna snart kommer ta egna genvägar för att lösa problem. Plötsligt känns det jobbigt att logga in med tvåstegsverifiering och viktiga affärsdokument mejlas från en privat e-postadress istället. Det är också vanligt att viktiga dokument sparas lokalt i datorn eller på en privat Google Drive, trots att arbetsplatsen har tydliga riktlinjer för användning av VPN eller cloudlösningar.

Så åtgärdar ni problemet:

- Ta fram och förankra policys internt för IT-säkerhet, lösenordshantering och lagring.
- Kräv tvåstegsverifiering för inloggning på e-post och andra viktiga program.
- Välj verifierade program från stora leverantörer som Microsoft för att öka säkerheten.
- Använd cloudlösningar för att förhindra användare att spara filer lokalt.
- Centralisera IT-miljön för att få full kontroll över företagets enheter, lösenord och användarrättigheter.
- Mobile Device Management-server (MDM) med tjänster som Jamf Pro hjälper dig reglera behörigheter, uppdatera mjukvara och spärra enheter som utgör en säkerhetsrisk.

KULLANDER

* https://home.kpmg/se/sv/home/nyheter-rapporter/2020/04/cyberattacker-okar-i-sparen-av-covid-19.html

** https://www.krisinformation.se/nyheter/2020/mars/folkhalsomyndigheten-uppmanar-till-distansarbete

RISKFAKTOR 2:

INTRÅNG

En ovan IT-organisation har sällan helt säkra lösningar för distansarbete, vilket ökar risken för cyberattacker och intrång. Det är vanligt att man använder externt åtkomliga tjänster med kända sårbarheter och att man arbetar via öppna nätverk. Många kriminella använder sig också av phishing och skickar mejl där mottagaren uppmanas att öppna en fil innehållandes en trojan som stjäl viktig information som lösenord. Men även om det finns mycket som ni kan göra internt för att förebygga och förhindra dataintrång, så vilar det största ansvaret på den enskilda användaren.

Så åtgärdar ni problemet:

- Sätt upp tydliga ramverk för datorns inställningar via en MDM-server. Kryptera hårddisken, ta bort eventuella gästkonton och begränsa möjligheterna att dela filer via nätverket. Enheter som bryter mot ramverket varnas eller blockeras.
- Förhindra användaren att installera vissa typer av program. Apple har till exempel byggt in programmet Gatekeeper i macOS, vilket gör att användaren enbart kan ladda ner program från AppStore och verifierade användare.
- Använd cloudbaserade lösningar med inbyggda säkerhetsmekanismer som tvåstegsverifiering.
- Välj säkra mötesprogram med krypterade anslutningar som Microsoft Teams för att kontrollera vem som närvarar.
- Utbilda användarna i IT-säkerhet för att skapa medvetenhet. Fokusera på vikten av att ha ett säkert lösenord, att förvara datorn på ett skyddat ställe och att alltid logga ut när datorn inte används.

RISKFAKTOR 3:

EN SLUTKÖRD IT-AVDELNING

Många anställda på IT-avdelningen upplever en stressig tillvaro och arbetsbördan minskar sällan när större delen av personalstyrkan sitter på hemmakontoret. Hur ska man hantera den stora mängden samtal och mejl om borttappade filer och krånglande datorer utan att tappa tålamodet? Och vad händer egentligen om flera nyckelpersoner på IT-avdelningen blir sjuka? En utmattad IT-avdelning kan snabbt bli ett hinder som försenar och försvårar det dagliga arbetet.

Så åtgärdar ni problemet:

- Våga ta hjälp av en extern IT-leverantör för att få avlastning där den behövs. I kristider handlar det framför allt om att någon svarar i andra änden och kan hjälpa eller lugna.
- Genom att centralisera IT-miljön är det enkelt för den interna eller externa IT-avdelningen att snabbt få en överblick över och åtgärda problem.
- Redundansen, d.v.s. feltoleransen, ska inte bli ett problem för IT-avdelningen. Se till att det finns back-up som garanterar att systemet fungerar även om något går sönder.