Ökade säkerhetsrisker när fler arbetar hemifrån – så skyddar ni era digitala tillgångar

För att begränsa smittspridningen av Coronaviruset väljer många svenska företag att låta sina anställda arbeta hemifrån. Med populära samarbetsverktyg som Microsoft Teams, Trello eller Slack kan de flesta företag snabbt ställa om till ett virtuellt arbetssätt. Omställningen kommer dock inte utan utmaningar. Med en stor mängd data som flyttas till potentiellt osäkra platser och medarbetare som sitter på privata eller osäkra Wi-fi-uppkopplingar kan företagens digitala tillgångar riskera att exponeras. Den nordiska IT- och digitaliseringspartnern Nordlo går här igenom de största riskerna – och lösningarna.

När stora delar av den svenska arbetsföra befolkningen nu jobbar hemifrån ställer det höga krav på företagen både gällande hur väl man samarbetar på distans, men också när det kommer till den digitala säkerheten. När många använder samarbetsverktyg, som exempelvis Microsoft Teams, flyttas en stor del av företagets data till platser i molnet som kan vara sårbara samtidigt som medarbetare ofta använder privata, kanske osäkra uppkopplingar. För att kunna säkra sina digitala tillgångar behöver företag vara medvetna om de största riskerna, och hur man bäst undviker dem.

– Vi är ganska väl rustade i Sverige ur ett kommunikationsperspektiv i och med att vi har ett väl utbyggt mobil- och fibernät. Många företag har under de senaste åren börjat använda moderna cloudplattformar för att samarbeta online vilket gör att man kan ha ett liknande arbetssätt hemma som på kontoret. Men, när vi arbetar virtuellt i högre utsträckning blir vår data också mer sårbar, berättar Jesper Neumann, Cloud Solution Architect på Nordlo.

”Ofta en varningsklocka”

En av de vanligaste riskerna är så kallad “social engineering” där företag och medarbetare kontaktas via mejl eller telefon och ombeds att exempelvis klicka på en länk, bekräfta ett bankkort eller betala en falsk faktura. Tumregeln är där att vara medveten och agera utifrån devisen att om något verkar för bra för att vara sant, så är det antagligen det, förklarar Jesper Neumann.

– Uttrycker personen som kontaktar en att det är väldigt bråttom är också det ofta en varningsklocka. Man ska aldrig klicka på okända länkar eller ringa okända nummer, utan istället kontakta sin egen bankkontakt eller hitta alternativa säkra kontaktuppgifter till personen som hört av sig.

En annan vanlig risk är lösenordskapningar. Stulna lösenord går idag att köpa i bulk online och när anställda använder ett och samma lösenord till flera system ökar risken att de hamnar i orätta händer. För att undvika att obehöriga kommer åt företagets data är multifaktorautentisering (MFA), som t ex mobilt BankID, den allra bästa lösningen.

– Vi rekommenderar alla våra kunder att använda MFA. Det minskar risken för lösenordskapning med 99,9 procent. I och med att mycket av företagens data ligger i molnet idag så räcker det inte med bara användarnamn och lösenord, man behöver ett extra skydd, säger Jesper Neumann.

Viktigt att uppdatera programvara

En av de enklare åtgärderna man kan genomföra för att skydda sin data är också en av de mest effektiva: att uppdatera sin programvara.

– När vi ser elaka saker som fått fäste i kunders miljöer är det ofta på grund av att man inte uppdaterat programvaran och att det finns säkerhetshål som inte är igentäppta. I större bolag sköts detta ofta av

företagets IT-avdelning medan det i mindre bolag är vanligt att användarna själva får sköta om detta. Säkerhetshålen kan exempelvis vara i en router eller i operativsystemet på en laptop eller telefon.

Nordlo hjälper organisationer med innovativa och hållbara IT-lösningar som skapar affärsvärde. Med ett stort fokus på rådgivning och lokal förankring på 37 orter i Sverige och Norge siktar koncernen på att bli Nordens ledande IT- och digitaliseringspartner. Inom området säkerhet ser Nordlo att många företag saknar kontinuitetsplaner för att säkerställa att verksamheten och IT-miljön är säkrad och tillgänglig vid olika typer av katastrofer – som exempelvis under den pågående Coronakrisen.

– Det har under de senaste tio åren skett en förflyttning där IT har gått från att stötta verksamheten till att vara direkt verksamhetskritisk och avgörande för företagets fortlevnad. När många nu arbetar hemifrån behöver verksamheten fungera lika bra och detta måste vara en del av kontinuitetsplanen för it, säger Magnus Blomberg, Teknisk chef på Nordlo.

Säkerställ skyddet proaktivt

Nordlo effektiviserar sina kunders verksamheter med hjälp av IT. En del i det arbetet består av att genomföra risk- och möjlighetsanalyser. Ofta är det enkla åtgärder som verksamheten kan vidta för att höja säkerheten, där planering är en nyckelfaktor.

– Det gäller att säkerställa att man har ett fullgott skydd och tillgänglighet vid kriser, attacker eller yttre påverkan som t ex naturkatastrofer. Då behöver man även ha dokumenterade processer och rutiner. Inget ska hänga på en enda person, utan kritiska lösenord och rutiner måste finnas tillgängligt vid behov, förklarar Magnus Blomberg.

När allt fler företag lägger kritisk data i molnet ställer det ännu högre krav på förberedelse. Problemen kring säkerhet och kontinuitet försvinner inte utan de flyttas bara. Man måste själv ställa sig frågan om informationen verkligen är säkrad och vad som händer vid en eventuell katastrof – kan man då fortsätta att bedriva sin verksamhet?

– Vi arbetar mycket med att stötta och ta fram rutiner för dessa ändamål. Är målet att ha en så säker verksamhet som möjligt så bygger vi lösningar utifrån kundunika säkerhetskrav. Det viktigaste är att man är proaktiv och också definierar en körplan om något trots allt går snett, dvs definierar vad som ska återställas först och vem som gör vad, avslutar Magnus Blomberg.

Länk till: https://nordlo.com/kontakt