5 tips – så skyddar du företaget mot dataintrång

Cyberattackerna ökar i tider av oro. Men det finns knep du kan ta för att skydda företaget. Det här ska du tänka på.

Oktober är europeisk informationssäkerhetsmånad, där Polisen, Skatteverket och andra myndigheter uppmärksammar cyberhot med kampanjen Tänk Säkert. Men dataintrång kan lika gärna ske när som helst. Något som är tydligt är att de har ökat i tider av covid-19.

– Vi har sett en ökad aktivitet av cybersäkerhetsincidenter, såsom intrång och attacker, under pandemin i takt med att organisationer och anställda kommit att bli mer sårbara när man arbetar på andra sätt. I tider av oror kan det utnyttjas, säger Sam Graflund Wallentin, specialist på cybersäkerhet på PwC.

För företagare gäller det att ständigt hålla ett vaksamt öga på verksamheten. Vissa perioder på året finns däremot en större risk att drabbas olika typer av oönskade IT-attacker. Att komma ihåg är även att när e-handeln ökar finns möjligheter för cyberkriminella att lura köpare på kortuppgifter, skicka falska fakturor men även skicka falska kampanjer som innehåller skadlig kod eller bilagor. Vanligast i den här typen av brottslighet är att luras via mejl.

– I slutet av året drabbas många. Men även på sommaren, då färre personer arbetar och frågor kring cybersäkerhet hamnar i skymundan. Just därför bör man se över rutiner kring tekniska system och medarbetarnas kompetens, påpekar Sam Graflund Wallentin.

5 tips – så skyddar du företaget mot dataintrång

1. Hur försvarar vi företaget från phishingattacker?
Skadlig kod och andra bedrägerier via mejl är en mycket vanlig ingångsväg varför det är viktigt att ha rutiner, medvetenhet och tekniska lösningar för att filtrera, upptäcka och hantera phishing-mejl. En oerhört allvarlig typ av skadlig kod som kan komma denna väg är ransomware, som i värsta fall kan stjäla data och kryptera hela IT-miljön och kräva lösensumma för att låsas upp.

2. Hur kontrollerar vi administratörskonton?
De som gör dataintrång vill åt byråns administratörsrättigheter, för då kan de komma åt de allra känsligaste uppgifterna och in i föetagets olika system och databaser. Fråga er: Hur kan vi begränsa användningen och bevaka dessa konton systematiskt?

3. Hur ser vi till att våra applikationer och enheter är uppdaterade?
Kan vi som företag mäta hur många av våra applikationer system och servrar som är uppdaterade och när det görs? Målet är att alla system alltid vara uppdaterat med det senaste.

4. Hur ser vi till att våra partners och leverantörer skyddar informationen vi delar med dem?
Alla verksamheter har på något sätt en relation till leverantörer, exempelvis IT-leverantörer. De behandlar vår och våra kunders information. Men man måste alltid fråga sig: Hur säkerställer vi att leverantörerna uppfyller säkerhetskraven? Vilket land sitter de i? Se till att ha standarder och att leverantörerna skickar säkerhetsrapporter.

5. Hur kontrollerar vi åtkomst till våra system och vår data?
Byrån behöver ha en ansats med hur man jobbar med administratörsrättigheter internt, det vill säga, med alla användarnas behörigheter och rättigheter till data och system. Man brukar prata om att principer om minsta behörighet ska styra och att man endast ska ha behörigheter för de uppgifter man utför. En annan handlar om att separera ansvar för

uppgifter. Exempelvis att inköp behöver attesteras av annan person än den som utför köpet. Ytterligare en aspekt avser hur anställdas behörigheter ska följa dess anställning, med andra ord, byter man roll eller slutar ska behörigheterna ändras.

Sofia Hadjipetri Glantz