Pressmeddelande
20 oktober 2025

Omedvetna AI-användare – en växande säkerhetsrisk

Det finns ett glapp mellan ledningens höga tilltro till den egna säkerheten och ett utbrett riskbeteende, inte minst när det gäller AI och nätfiske. Det visar en ny undersökning som belyser den mänskliga faktorn inom cybersäkerhet.

Arctic Wolf, ledande inom operativ cybersäkerhet, presenterar 2025 Human Risk Behavior Snapshot, den andra årliga undersökningen om riskbeteende som nu genomförts bland över 1 700 IT-beslutsfattare och användare, med medverkan från de nordiska länderna.

Samtidigt som företag och organisationer fortfarande har hög tilltro till sin säkerhet så visar undersökningen på en fortsatt hög hotaktivitet där många incidenter och intrång beror på enkla vardagliga misstag av medarbetare. Nätfiske genom bluffmeddelanden är fortfarande en av de vanligaste orsakerna till dataintrång. Samtidigt ökar AI-användningen, och med den riskerna för exponering av känsliga uppgifter genom omedvetna medarbetare.

Att AI blivit en del av vardagen på arbetsplatsen gör det allt svårare att bedöma den mänskliga faktorn och dess betydelse för cybersäkerheten. Många chefer har ett överdrivet förtroende för den egna säkerheten samtidigt som anställda kringgår eller missbrukar grundläggande säkerhetsåtgärder. Då uppstår ett glapp mellan upplevd och verklig riskexponering.

– Generativ AI ger oss kraftfulla nya verktyg, men tillför också kraftfulla nya risker. När ansvariga chefer förbiser hur anställda faktiskt använder tekniken skapar det perfekta förutsättningar för intrång som orsakas av mänskliga misstag. För att minska dessa risker är det viktigt att ledningen inser att det handlar om ett ansvar som måste tas och delas genom hela organisationen, liksom att bygga en kultur där medarbetarna har möjlighet att säga ifrån, lära av misstag och kontinuerligt förbättra sig, säger Adam Marrè, vice VD och informationssäkerhetschef (CISO) på Arctic Wolf.

Arctic Wolfs Human Risk Behavior Snapshot syftar till att hjälpa beslutsfattare och säkerhetsteam att identifiera utmaningarna och hantera riskerna kopplade till den mänskliga faktorn som finns i varje organisation. Några slutsatser i rapporten:

- **Dataintrång ökar globalt:** 68% av IT-cheferna uppger att deras organisation drabbats av dataintrång under det senaste året – en ökning med 8% från 2024. Siffran för Norden ligger på 71%, över genomsnittet globalt och en betydande ökning jämfört med 2024 (60%).
- **Nätfiske lurar även experterna:** Nästan två tredjedelar av IT-cheferna och hälften av de anställda erkänner att de klickat på skadliga länkar, men tre fjärdedelar av ledarna tror fortfarande att deras organisationer är säkra.
- **Utsatta chefer:** Ledningsgrupper fortsätter att vara ett huvudmål för attacker. 39% har drabbats av nätfiskeförsök och 35% för angrepp med skadlig kod.
- **AI-användning skapar risker för dataläckor:** 80% av IT-cheferna och 63% av de anställda använder verktyg för generativ AI i sitt arbete. 60% av ledarna och 41% av personalen erkänner att de matar dessa verktyg med interna data.
- **Grundläggande säkerhet försummas:** Exempelvis är det bara 54% av organisationerna som tillämpar flerfaktorsautentisering för alla användare. Med enkla och ofta svaga lösenord lämnas konton oskyddade och öppnar för intrång.

Arctic Wolfs rapport visar att mänskliga riskfaktorer är en växande utmaning globalt – och inte minst i Norden, där andelen organisationer som har upplevt ett dataintrång under det senaste året har ökat från 60 procent till 71 procent. Utvecklingen understryker att säkerhet inte kan lösas enbart med teknik.

Risker drivs till stor del av mänskligt beteende – från nätfiskefel och svaga lösenord till oavsiktlig delning av konfidentiell data i AI-verktyg. De mest motståndskraftiga organisationerna är de som lyckas kombinera tekniska säkerhetsåtgärder med löpande fortbildning och en stark säkerhetskultur i hela företaget.

Om undersökningen

2025 Human Risk Behavior Snapshot bygger på två parallella undersökningar bland 855 IT-och säkerhetschefer på ledningsnivå och 855 slutanvändare (mellanchefer och högre chefer). De genomfördes med nätbaserade enkäter av Sapio Research i juli 2025 bland företag med över 50 anställda i 17 länder.

Mer information:

- Ladda ner hela rapporten 2025 Human Risk Behavior Snapshot från Arctic Wolf.
- Blogginlägg av Adam Marrè, CISO på Arctic Wolf där han kommenterar resultaten.
- Diskutera med Arctic Wolf på Facebook, X, LinkedIn och YouTube.
- Besök arcticwolf.com och ta reda på mer om våra lösningar för operativ säkerhet och ändpunkter.

Mediakontakt

Fredrik Pallin
Digital PR
fredrik@digitalpr.dk

Om Arctic Wolf

Arctic Wolf är en global ledare inom operativ cybersäkerhet som hjälper företag att minska riskerna med cyberattacker genom sin molnbaserade säkerhetsplattform. Arctic Wolfs Aurora-plattform bygger på öppen XDR-arkitektur och förenar kraften hos artificiell intelligens med världsledande säkerhetsexpertis för att erbjuda övervakning, åtgärder och riskhantering dygnet runt.
Vi får säkerhet att fungera!
www.arcticwolf.com