Ett av fem företag har betalat eller skulle betala lösensumma för sin information, konstaterar Thales

Ny forskning från Thales har funnit att ransomware fortsätter att plåga företag och myndigheter. Faktum är att 21 procent har upplevt en ransomware-attack under det senaste året. 43 procent av dem upplever att det haft en betydande påverkan på verksamheten.

- Världens IT-ansvariga rankar malware, ransomware och phishing som de vanligaste attackerna mot IT-säkerheten
- Mindre än hälften av företagen (48 %) har en formell ransomware-plan
- Dataintrång förblir vanliga och närmare en tredjedel (29 %) har upplevt ett dataintrång under de senaste 12 månaderna
- 79 procent av företagen uttrycker oro över säkerhetsriskerna med en allt mer distansarbetande arbetsstyrka
- 51 procent av IT-cheferna är överens om att det är svårare att hantera integritets- och dataskyddsbestämmelser i molnmiljö

Första gången ransomware upptäcktes var i slutet av 1980-talet med PC Cyborg viruset. Sedan dess har frekvensen och effekten av ransomware-attacker accelererat, inte minst på grund av ökningen av kryptovaluta som föredragen betalningsmetod. Faktum är att **2022 Thales Data Threat Report**, genomförd av 451 Research som intervjuat 2700 IT-beslutsfattare, fann att 22 procent av företag och organisationer i världen har erkänt att de har betalat eller skulle betala en lösensumma för sina data. Trots detta sa 41 procent av de tillfrågade att de inte planerar att ändra säkerhetsutgifterna, även med större effekter av ransomware-attacker.

Dessutom har 48 procent implementerat en formell ransomware-plan. Sjukvården är bäst förberedd med 57 procent som har en formell ransomware-plan medan energisektorn är minst förberedd där bara 44 procent av organisationerna har en plan. Detta trots att båda sektorerna har upplevt betydande intrång under de senaste tolv månaderna.

Data Visibility är en utmaning

I takt med att fler företag väljer en multimolnstrategi och mer arbete hemifrån förblir normen, tvingas de IT-ansvariga att försöka kontrollera utspridningen av informationen och får svårare att allt hitta data. 56 procent av de IT-ansvariga var mycket säkra eller hade fullständig kunskap om var datan lagrades, vilket är en minskning från 64 procent under föregående och endast 25 procent uppgav att de kunde klassificera all information.

Utmaningar, hot och efterlevnad

Under hela 2021 var säkerhetsincidenterna fortsatt höga då 29 procent av företagen upplevde intrång under det senaste året. Dessutom erkände 43 procent av de IT-ansvariga att de hade misslyckats med att följa upp efterlevnaden.

Globalt sett rankade de IT-ansvariga skadlig programvara (56 %), ransomware (53 %) och nätfiske (40 %) som de viktigaste orsakerna till säkerhetsattacker. Att hantera dessa risker är en pågående utmaning, där 45 procent av de IT-ansvariga rapporterar en ökning av volymen, svårighetsgraden och/eller omfattningen av cyberattackerna under det senaste året.

Molnet ökar komplexiteten och risken

Molnanvändningen ökar och 34 procent av de tillfrågade använde mer än 50 stycken Software as a Service-appar (SaaS) medan 16 procent använde mer än 100 appar. 51 procent av de IT-ansvariga instämde i att det är mer komplext att hantera integritets- och dataskyddsbestämmelser i en molnmiljö än i lokala nätverk inom, vilket är en uppgång på från 46 procent förra året.

Thales DataThreat Report 2022 visade också en betydande strävan bland företag att lagra data i molnet. 32 procent av de tillfrågade som uppgav att ungefär hälften av deras arbete och data finns i externa moln, och 23 procent som rapporterar att mer än 60 procent finns i molnet. Däremot rapporterade 44 procent att de hade upplevt ett intrång eller misslyckats med en revision i sina molnmiljöer.

Dessutom är användningen av kryptering för att skydda känsliga uppgifter låg, med 50 procent av de tillfrågade som avslöjar att mer än 40 procent av deras känsliga uppgifter har krypterats, och (22 procent uppger att mer än 60 procent har krypterats. Detta representerar fortfarande en betydande pågående risk för många organisationer.

Distansarbete oroar

Ytterligare ett helt år med distansarbete visade att hantering av säkerhetsrisker är en betydande utmaning för många organisationer. Majoriteten av företagen, 79 procent är fortfarande oroade över säkerhetsrisker och hot förknippade med distansarbete. Endast 55 procent av de IT-ansvariga rapporterade att de hade implementerat multifaktorautentisering (MFA), vilket är oförändrat från föregående år[1].

Hot vid horisonten

Rapporten visade också att IT-cheferna har många säkerhetsprioriteringar – vilket tyder på att de menar allvar med att ta itu med komplexa hotmiljöer. 26 procent uppgav att breda satsningar på verktyg för molnsäkerhet är den största framtida prioriteringen. Dessutom uppgav 25 procent av de IT-ansvariga att de prioriterade key management, med Zero Trust som en viktig strategi för 23 procent.

De IT-ansvariga är också allt mer medvetna om de framtida utmaningar som väntar. När de ombads identifiera säkerhetshot från quantum computing, sa 52 procent att de var oroliga över "morgondagens dekryptering av dagens data", en oro som sannolikt kommer att öka med den ökande komplexiteten i molnet.

Sebastien Cano, Senior Vice President for Cloud Protection och Licensing activities på Thales, kommenterar: *"När pandemin fortsätter att påverka både yrkeslivet- och privatlivet, har alla förväntningar om en "återgång" till pre-pandemiförhållanden bleknat. Medan team runt om i världen har fortsatt att klara utmaningarna i att säkra sina data, indikerar våra resultat att det behövs brådskande åtgärder för att utveckla mer robusta cybersäkerhetsstrategier. Attackerna, såväl som utmaningarna, kommer bara att öka under det kommande året, därför är det viktigt att implementera en robust säkerhetsstrategi baserad på upptäckt, skydd och kontroll."*

Thales och 451 Research kommer att diskutera rapportens resultat mer i detalj vid ett webinarium den 31 mars 2022. Om du vill delta, anmäl dig på registreringssidan. Individuella siffror för ett flertal länder inklusive **Sverige** finns redovisade i bifogat material.

Om the 2022 Thales Global Data Threat Report 2022

Thales Global Data Threat Report 2022 baserades på en global undersökning genomförd av 451 Research under januari 2022 och beställd av Thales där mer än 2 700 chefer med ansvar för eller inflytande över *IT and IT-säkerhet medverkar. Intervjupersonerna kom från 17 länder: Australien, Brasilien, Kanada, Frankrike,* Tyskland, Hong Kong, Indien, Japan, Mexiko, Nederländerna, Nya Zealand, Singapore, Sydkorea, **Sverige**, Förenade Arab Emiraten, Storbritannien och USA. Organisationerna representerade ett antal branscher med ett särskilt fokus på Life Science, finansiella tjänster, handel, teknik och myndigheter. Yrkestitlarna omfattade ledningspersonal som vd, CFO, CIO, CISO, Chief Data Scientist, riskansvarig, IT-chef, administratör, säkerhetsanalytiker, säkerhetsingenjör och systemadministratör. De tillhörde i sin tur organisationer av många olika storlekar med fokus på 500 till 10,000 anställda.

Presskontakt

Thales, Media Relations
Digital Identity and Security
Vanessa Viala
+33 (0)6 07 34 00 34
vanessa.viala@thalesgroup.com

Om Thales

Thales (Euronext Paris: HO) är världsledande inom avancerad teknik och digitala och "deep tech"-innovationer – uppkoppling, big data, artificiell intelligens, cybersäkerhet och kvantberäkning – för att bygga en trygg framtid som är avgörande för utvecklingen av våra samhällen. Koncernen förser företag, organisationer och regeringar med försvars-, flyg- och rymdteknik samt tekniklösningar för transport och digital identitet.

Thales har 81 000 anställda i 68 länder. Under 2020 omsatte koncernen 17 miljarder euro. https://www.thalesgroup.com/en