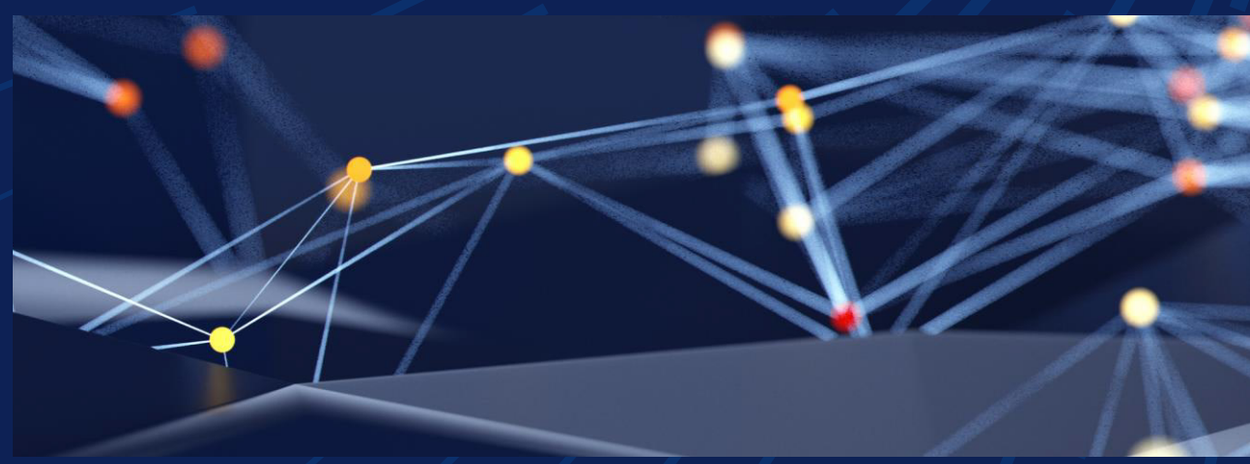
Cybersäkerhetens framtid:

Att anpassa sig till en ny digital era



Medan cybersäkerhetsexperter ofta är helt fokuserade på att förebygga attacker och utarbeta återställningsplaner, utvecklas den övergripande säkerhetsmiljön ständigt. Därför är det viktigt att planera för vad som kommer härnäst.

När vi blickar framåt är det tre områden som sticker ut: postkvantumkryptografi, förändrade regelverk och nya hot. Organisationer bör agera nu genom att planera och implementera lösningar när de är tillgängliga.

Gryningen för postkvantumkryptografi

Kvantberäkning har potential att förändra industrier genom att erbjuda enastående beräkningskraft som kan lösa problem långt bortom klassiska datorers räckvidd. Samma kraft kan dock göra nuvarande kryptografiska metoder föråldrade. Algoritmer som RSA och ECC, som ligger till grund för mycket av dagens säkra kommunikation, skulle kunna knäckas på några sekunder av en tillräckligt avancerad kvantdator. Denna hotbild har ökat behovet av postkvantumkryptografi.

Postkvantumkryptografi (PQC) handlar om att utveckla kryptografiska algoritmer som förblir säkra i en era av kvantberäkning. NIST (National Institute of Standards and Technology) har insett denna överhängande risk och leder arbetet med att standardisera kvantresistenta algoritmer.

För företag är förberedelser för denna övergång inte förhandlingsbara. Tidig implementering av PQC-lösningar säkerställer att data förblir säkra även när motståndare får åtkomst till kvantberäkning.

Som Bobbie Stempfley, VP of Cybersecurity och Business Unit Security Officer på Dell påpekar, bör organisationer inleda processen genom att fokusera på två viktiga områden:

Identifiera och inventera alla kryptografiska modeller som för närvarande används.

Tänk på in-flight data, inte bara data i vila. Tänk på nyckelhantering, kodsignering, enhetsidentifiering, säker åtkomst och telemetri. Skapa en omfattande inventering och skapa sedan en handlingsplan.

Förstå leverantörernas status.

Eftersom moderna företag kan ha tusentals leverantörer bör man vara medveten om de risker som dessa kan medföra. Arbeta för att säkerställa att även de planerar inför förändringen.

Utöver dessa utgångspunkter bör du genomföra riskbedömningar för att identifiera sårbara system, överväga att implementera hybridkryptografiska modeller för att kunna fortsätta driften under övergången och samarbeta med leverantörer som redan utforskar kvantsäkra lösningar. Tänk dock på att det inte finns någon leverantör eller teknik som erbjuder en färdig lösning.

Regelförändringar i en globaliserad värld

En annan viktig faktor som påverkar cybersäkerhetens framtid är det föränderliga regelverket. Regelverk sträcker sig nu långt bortom efterlevnad – de håller på att bli ett viktigt ramverk för att införa ansvarsskyldighet, driva på tekniska uppgraderingar och skydda medborgarna i en sammankopplad, datadriven värld. Utvecklingen går dock snabbt och varierar kraftigt mellan olika geografiska områden, vilket ökar komplexiteten i efterlevnaden.

Med detta sagt går dessa regelverk längre än bara påföljder för bristande efterlevnad – de fungerar som katalysatorer för bättre cybersäkerhetsrutiner. Företag som aktivt anpassar sina policyer efter regelverkets krav kan uppnå nya nivåer av förtroende och operativ effektivitet. För att uppnå detta bör organisationer upprätta styrningsramverk som är tillräckligt flexibla för att kunna anpassas till lagändringar, genomföra regelbundna efterlevnadskontroller och investera i utbildning för anställda så att de kan hantera känslig information i enlighet med de senaste standarderna.

När säkerhetschefer förbereder sig för efterlevnad är det viktigt att de ser till att de är begripliga och förstådda. Alltför ofta talar säkerhetsexperter i säkerhetstermer, vilket kanske inte går hem hos kunder, tillsynsmyndigheter och andra intressenter. Det är säkerhetsexperternas ansvar att se till att de blir förstådda, inte lyssnarnas att tolka dem.

> Tänk på övergången till postkvantumkryptografi som att flytta ett fullt möblerat hus. Det kommer bli lika komplicerat och utmaningen är att inte förstöra något under processen.”
>
> ***Bobbie Stempfley***
> *VP, Cybersecurity and Business Unit Security Officer, Dell Technologies*

Utvecklingen av hotbilden (och försvaret)

AI revolutionerar företag, ökar produktiviteten och öppnar upp nya möjligheter för mänsklig potential. När det gäller cybersäkerhet gynnar AI både skadliga aktörer och försvarare:

Fientlig användning: AI möjliggör mer sofistikerade attacker, till exempel mycket övertygande spear phishing-attacker och deepfake-bedrägerier.

Defensiv användning: AI hjälper försvarare genom att:

- Bearbeta stora mängder säkerhetsdata snabbt.
- Prioritera hot på ett mer effektivt sätt.
- Förbättra detekterings- och svarsfunktioner.

Säkerhetsverktygen kommer fortsätta att förbättras, men med hjälp av naturlig språkbehandling kan säkerhetsexperter kommunicera mer direkt med sina system och ge systemen möjlighet att proaktivt vidta korrigerande åtgärder för cybersäkerhet.

Organisationer bör sträva efter att samtidigt utnyttja dessa möjligheter och se till att deras utbildning och andra försvarsmekanismer hålls uppdaterade. Utbildning är det bästa sättet att förhindra att anställda faller offer för mer sofistikerade attacker.

Att bli lösenordsfri

Lösenord är inte längre den säkraste metoden för identitets- och åtkomsthantering.

Traditionella lösenordsbaserade system har betydande sårbarheter, vilket gör dem till en alltmer otillräcklig lösning för moderna cybersäkerhetsbehov. Lösenord är känsliga för attacker som credential stuffing, nätfiske och brute-force-försök, vilket ofta utsätter organisationer för onödiga risker. Dessutom förvärras dessa sårbarheter av dåliga användarvanor, såsom att återanvända lösenord eller skapa svaga lösenord.

Dessutom förvärras dessa sårbarheter av dåliga användarvanor, som att använda samma lösenord flera gånger eller skapa svaga lösenord. Övergången till lösenordsfria system innebär en avgörande utveckling inom identitets- och åtkomsthantering, där säkerhetsåtgärderna anpassas till de alltmer sofistikerade cyberhoten.

Att införa lösenordsfria tekniker ger också många fördelar, bland annat minskad attackyta, förbättrad användarupplevelse genom snabbare och smidigare inloggningar samt lägre IT-kostnader genom färre lösenordsrelaterade incidenter. Användningen av avancerade metoder säkerställer en starkare säkerhetsställning och hjälper organisationer att uppnå efterlevnad av regleringsstandarder. Övergången till lösenordsfria system är inte bara en trend utan ett nödvändigt steg mot att skapa ett säkrare och effektivare digitalt ekosystem för både individer och organisationer.

Sammanfattning

Cybersäkerhet går in i en omvälvande era, präglad av kvantberäkning, förändrade regleringar och allt mer sofistikerade hot. För att ligga i framkant måste organisationer använda innovationer som postkvantumkryptografi, AI-drivna försvarssystem och lösenordsfri autentisering. Genom att prioritera beredskap, samarbete och strategiska investeringar kan företag skapa en säkrare och mer motståndskraftig digital miljö. Du har ingen tid att förlora.

Dell-produkter och -lösningar som kan hjälpa dig

Utvalda Dell-lösningar	Beskrivning
Rådgivningstjänster för cybersäkerhet	Experthjälp som kan hjälpa dig att planera för det föränderliga hotlandskapet, inklusive aktuella och nya hot.
vCISO	Chef för virtuell informationssäkerhet och cybersäkerhetsexpert som kan hjälpa till att identifiera och hantera risker samt vägleda strategiska beslut.

Lär dig att hantera några av dagens främsta cybersäkerhetsutmaningar på **dell.com/cybersecuritymonth**

DELL Technologies