Microsoft 365

Bästa praxis som rör dataskydd:

Hur Microsoft 365 hjälper er att skydda era data

Innehålls-förteckning

Cyberrymden: företagens nya slagfält

Digitaliseringen har gjort att mängden data som genereras på företagets olika avdelningar formligen har exploderat. Dessa data kan vara i många format, däribland konfidentiell affärsinformation, t.ex. företagets ekonomi, känslig eller personligt identifierbar information, t.ex. personnummer eller privilegierad kontoinformation, t.ex. autentiseringsuppgifter och lösenord.

Den känsliga naturen av så mycket data gör den till en viktig affärstillgång som måste skyddas. Fragmenterade tekniklösningar, brist på tydligt ägarskap till dataskyddsansvar och begränsade resurser skapar emellertid utmaningar för organisationerna när de skyddar sina data.

Cyberangrepp och intrång blir allt vanligare och kan få allvarliga konsekvenser.

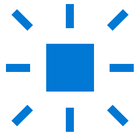
46 %

En nyligen genomförd undersökning visar att 46 procent av organisationerna drabbades av skador på deras anseende och varumärkesvärde till följd av ett cyberintrång.[1]

[1] "De aspekterna av IT-risk och -rykte," TechRepublic, 2013. Nämns i "Följdverkningar: IT-riskens påverkan på anseendet," Forbes Insights, 2014.

Ett starkt integritets- och säkerhetsprogram skyddar inte bara din organisation från skadliga intrång, utan låter dig även ta del av kraftfulla konkurrensfördelar, inklusive:

Efterleva dataskyddslagar (dvs. the EU:s allmänna dataskyddsförordning).



Förbättrat varumärkesvärde.

Ökat förtroende bland kunder, medarbetare och intressenter.

- Den höga synligheten av moderna angrepp har höjt datasäkerheten från en konversation inom IT-avdelningen till en konversation på styrelsenivå. IT-säkerhetschefer spelar en viktig roll när det gäller att leda denna konversation.
- I den här e-boken beskrivs de bästa metoderna för dataskydd, däribland tekniska lösningar som hjälper er att skydda känsliga data och minska risken för att de hamnar i fel händer.

Eftersom digital störning förändrar det konkurrenskraftiga landskapet i alla större branscher, kommer sättet som företagen samlar in, bearbetar och agerar på data att vara avgörande för deras framgång. Utan utvecklade säkerhetsfunktioner kommer företagen att stå hjälplösa inför komplicerade regelkrav och löpa ökad risk för att bli utsatta för cyberangrepp."

Forrester[2]

[2] "Utvärdera din cybersäkerhet och sekretessmognad," Forrester, 2020.

Bästa praxis som rör dataskydd

Ett starkt dataskydd- och säkerhetsprogram är inte en engångslösning. Det är något du kontinuerligt främjar hos de människor, processer och tekniker som din organisation utgörs av.

Genom att använda följande bästa praxis kan du hjälpa till att göra dataskydd till en integrerad del av ditt arbetssätt.

1. Skapa en styrkommitté för dataskydd
2. Kämpa för en kultur med ansvarsfull dataanvändning
3. Socialisera era policyer, utbilda medarbetarna
4. Granska era data och håll er uppdaterade om kraven
5. Kontrollera och testa regelbundet programmets effektivitet
6. Använd smidiga verktyg för att maximera effektiviteten

1 Skapa en styrkommitté för dataskydd

För många organisationer är det oklart vem som bär ansvaret för dataskydd. Det är viktigt med dataskydd för alla juridiska-, efterlevnads- och IT-avdelningar och även för företagsgrupper. Detta kan emellertid leda till isolerade tankegångar och luckor i dataskyddsstrategier.

Skapa samordning mellan olika avdelningar genom att bilda en styrgrupp som består av lämpliga intressenter. Detta hjälper till att säkerställa att dataskyddspolicyer och responsplaner för incidenter är omfattande och meddelas tydligt inom hela organisationen.

2 Kämpa för en kultur med ansvarsfull dataanvändning

C-suite-ledare är avgörande när det gäller att skapa en företagskultur som värdesätter dataskydd. Företagsledare kan vara ett gott föredöme för medarbetare på alla nivåer genom att anamma ett tankesätt om dataskydd och tydligt meddela att dataintegritet är en strategisk prioritet. Denna kultur av ansvarsfull dataanvändning bör även gälla för leverantörer, konsulter och andra tredje parter.

En ny rapport från Forrester understryker vikten av företagskultur: ”Dina policyer, rutiner och kontroller har begränsad effektivitet om organisationen saknar säkerhetskultur och datamedvetenhet. Hjälp till att ge medarbetarna möjlighet att göra det rätta och förstå vad de ska göra för att samla in och hantera data på ett lämpligt sätt.”[3]

[3] “Framtiden för datasäkerhet och integritet: Tillväxt och konkurrenskraftig differentiering,” Forrester, 2019.

3 Socialisera era policyer, utbilda medarbetarna

För att ert dataskyddsprogram ska vara effektivt måste policyer kommuniceras tydligt på alla nivåer. Om medarbetarna inte helt känner till eller förstår dem kan de inte följa dem. Insiderhot, oavsett om de är avsiktliga eller inte, är den vanligaste orsaken till dataintrång för organisationer av alla storlekar och dessa intrång är dyra. Enligt en studie utförd av Ponemon Institute kostar varje incident relaterad till en vårdslös medarbetare eller entreprenör i genomsnitt 283 281 USD.[4]

Minska risken för insiderhot genom att göra mer än att skicka ett meddelande eller en engångsutbildning. Effektiv utbildning innebär upprepad kommunikation, frekventa uppdateringar och vägledning när problem uppstår. Förvara dessutom alla relevanta policyer i ett omfattande dokumentlager som uppdateras regelbundet och som medarbetarna alltid har tillgång till.

[4] "2018 Kostnaden för insiderhot: Globalt," Ponemon Institute (sponsrad av ObserveIT), 2018.

4 Granska era data och håll er uppdaterade om kraven

En viktig del av alla dataskyddsprogram är att förstå de olika dataskyddskraven och säkerhetskraven du står inför och hur de tillämpas på din organisations data. Dessa krav kan styras av kunder, din organisations egna policyer, eller de kan vara av lagstiftningskaraktär. För starkt reglerade branscher som hälso- och sjukvård, finansiella tjänster eller tillverkning, eller för företag som verkar i flera jurisdiktioner, kan lagstiftningen vara ganska komplicerad.

När du väl har förstått de olika kraven och fått en fullständig bild av din organisations data och hur information tas emot, utnyttjas, hanteras och vidarebefordras, kan du utvärdera din organisations befintliga datasekretess- och säkerhetsprogram och hitta potentiella områden som kan förbättras.

5 Kontrollera och testa regelbundet programmets effektivitet

Utvärdera effektiviteten i dina dataskyddspolicyer och identifiera proaktivt områden med potentiell risk genom att löpande övervaka och testa. Ett bra sätt att tänka på övervakning är att betrakta den som ett tidigt varningssystem som varnar dig för potentiella data- och säkerhetsproblem innan de blir skadliga.

Tidigare var övervakning en resurskrävande funktion, men framstegen inom artificiell intelligens och automatisering gör nu övervakning enklare än någonsin. Automatisering av övervakningsrelaterade uppgifter som annars skulle göras manuellt hjälper inte bara att frigöra kritiska IT-resurser, de hjälper dig också att upptäcka hot snabbare och mer exakt.

6 Använd smidiga verktyg för att maximera effektiviteten

Fragmenterade lösningar för att hantera data inför komplexitet i processen och gör det svårare för organisationer att skydda känsliga data. I nyligen genomförd undersökning av IT- och säkerhetschefer rapporterar 44 procent av organisationerna att komplexiteten är det främsta hindret för bra datasäkerhet.[5]

Effektiviserade verktyg för datahantering och övervakning kan hjälpa er att:

- **Automatisera identifiering och klassificering av data** för att stödja efterlevnad och minska risken för intrång.
- **Hantera styrning av nätverkstjänster** för att inkludera problem som fjärråtkomst, enhetshantering och säkerhetskopiering och haveriberedskap.
- **Kryptera känsliga data** så att den är oläsbar för eventuella tredje parter som kan få tillgång till den.
- **Skydda IT-infrastruktur** från potentiellt illasinnade aktörer med sårbarhetsgranskning och korrigering.

[5] "25 viktiga statistiska uppgifter för datasäkerhet," Tech Beacon, 2019.

Varför Microsoft 365 ES

När organisationer antar beprövade, lättanvända lösningar för datahantering kan medarbetarna jobba mer effektivt och de ledare som är ansvariga för dataskydd kan fokusera på att integrera bästa praxis som beskrivs ovan.

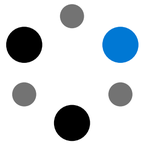
Microsoft 365 är en omfattande företagslösning som tillhandahåller tillförlitligt skydd i företagsklass.

- Skydda åtkomsten till dina data. Microsoft 365 använder Azure Active Directory för att hantera användaridentiteter bakom kulisserna. Windows Hello för företag Business ersätter lösenord med stark flerfaktorautentisering i Windows 10. Och Microsoft 365 Enterprise E5 identitets- och åtkomsthanteringslösningar förser dig med den intelligens du behöver för att identifiera riskabelt inloggningsbeteende och ger möjlighet att tillämpa policyer som begränsar eller blockerar åtkomst beroende på angivna regler.

- Skydda din information. Teknik för informationsskydd i Microsoft 365 som standard hjälper till att säkerställa att viktiga data förblir säkra och att endast de rätt personerna får tillgång till den. Microsoft 365 gör att användare kan sömlöst skicka krypterad och rättighetsskyddad e-post för att förhindra att känsliga data i dokument och e-postmeddelanden delas på olämpligt sätt. Du kan också kontrollera åtkomst med flexibla, anpassningsbara policyer.

- Försvara mot cyberhot. Tekniken för skydd mot hot i Microsoft 365 hjälper till att skydda mot och ge insyn i skräppost, skadliga program, virus, försök till nätfiske, skadliga länkar och andra hot.

Unika produktsärskiljare omfattar:



Integrerade lösningar som går längre än dagens punktlösningar, till exempel Microsoft Threat Protection och Microsoft Information Protection.

Intelligent Security Graph som bearbetar över 6,5 biljoner signaler varje dag för att skydda mot ständigt föränderliga avancerade angrepp.

Integritet, säkerhet och efterlevnad är viktiga för Goodyear. Med Microsoft 365 har vi förbättrat vår förmåga att hantera säkerhet och skydda våra data och immateriella rättigheter. En av de största delarna av det ekosystemet är Windows 10 – en högsta prioritet för att modernisera och stärka skrivbordet. Idag har vi kommit betydligt längre när det gäller att hantera cybersäkerhet än tidigare."

Sherry Neubert
Chief Information Officer
Goodyear Tire & Rubber Company[6]

[6] "Goodyear stärker arbetsstyrka och påskyndar fordonsinnovation med intelligenta verktyg i Microsoft 365," Microsoft, 2019.

Göra att Microsoft 365 E5 fungerar för dig

Upptäck hur Microsoft 365-företagslösningar kan hjälpa dig att skapa ett starkt ramverk för dataskydd för din organisation.

Kontakta en säljare