Lösningsguideserien

Microsoft

Säkerhet:
Guide till att skapa motståndskraft

Utforska säkerhetsmål

Stärka säkerheten

Hotlandskapet utvecklas, och ett växande antal angreppsytor har överbelastat resurserna inom cybersäkerhet och resulterat i utarbetade team. För att skapa motståndskraft i organisationen behöver säkerhetsteamet få tillgång till lösningar som förser dem med omfattande information om hot.

Möt dagens utmaningar med integrerade lösningar för samtliga användare, enheter, appar och data. Arbeta enkelt på olika plattformar med inbyggda upplevelser. Och skydda företagets framtid med AI och automatisering.

I den här guiden får du anvisningar om hur du steg för steg kan skydda din organisation och samtidigt skapa en smidig användarupplevelse, så att användarna får jobbet gjort. Varje scenario innehåller en kort lista med frågor, rekommenderade aktiviteter och resurser för att komma igång.

Säker fjärråtkomst

Ge distansarbetare möjlighet att komma åt de appar de behöver var och när som helst, med förbättrad säkerhet.

Användbara frågeställningar	Rekommenderade aktiviteter
1. Har ni en metod för att hantera identiteter på alla enheter och i alla appar?	☐ Använd Microsoft Azure Active Directory (Azure AD) som universell identitetsplattform.
2. Kan användarna logga in och smidigt komma åt alla affärsappar?	☐ Använd enkel inloggning med Azure AD, så att medarbetarna kan komma åt resurser från alla appar eller enheter när de jobbar på distans.
3. Använder ni för närvarande lösenord vid autentisering?	☐ Använd Microsoft Azures multifaktorautentisering för att höja säkerheten vid distansarbete.
4. Kan ni utöka säkerheten även till enheter?	☐ Hantera och skydda företagsdata i godkända appar på personliga enheter med hjälp av Azure AD och Microsoft Endpoint Manager.

Kom i gång med de här resurserna:

- Kom igång med en snabbkurs i Azure Active Directory.
- Lär dig mer om att skydda distansarbetare.
- Kom igång med att använda säkra lösningar för distansarbete.

Eliminera VPN-flaskhalsar

Lägg till nya identitetsbaserade kontroller i det befintliga nätverket för att förhindra störningar i verksamheten och återinförande av gamla risker.

Användbara frågeställningar	Rekommenderade aktiviteter
1. Hanterar du säkerheten för alla molnappar som din organisation använder?	☐ Håll reda på vilka molnappar som används i organisationen och skydda dem med funktioner som enkel inloggning och villkorsstyrd åtkomst i Microsoft Cloud App Security och Azure AD.
2. Har ni stöd för villkorsstyrd åtkomst baserad på identitet?	☐ Använd villkorsstyrd åtkomst som en del av Azure AD.
3. Hanterar du säkerheten för alla molnappar som din organisation använder?	☐ Håll reda på vilka molnappar som används i organisationen och skydda dem med funktioner som enkel inloggning och villkorsstyrd åtkomst i Microsoft Cloud App Security och Azure AD.
4. Hur kan ni gå över till en lösning med enkel inloggning till alla appar i molnet och lokalt?	☐ Skydda åtkomsten till äldre appar med Azure AD App Proxy, eller fördefinierad integration med nätverksleverantörer och appleveranskontrollanter.

Kom i gång med de här resurserna:

- Se webbseminariet Säkerhetskontroller för distansarbete.
- Läs whitepapret Enkel inloggning och hanterad åtkomst till alla appar från molnet.
- Lär dig mer om säkert distansarbete.

Kom igång med Noll förtroende

Noll förtroende bör betraktas som en integrerad säkerhetsfilosofi. Det är både en process och själva grunden för säkert distansarbete.

Användbara frågeställningar	Rekommenderade aktiviteter
1. Har ni en identitetslösning som omfattar villkorsstyrd åtkomst och analys för att förbättra insynen?	☐ Verifiera och säkra varje identitet med stark autentisering överallt.
2. Beviljas åtkomst endast till godkända enheter som hanteras i molnet?	☐ Få insyn i vilka enheter som ansluter till nätverket. Säkerställ efterlevnad och hälsostatus innan åtkomst ges.
3. Konfigureras molnappar och lokala appar som ansluts till internet med enkel inloggning?	☐ Upptäck skugg-IT, begränsa åtkomsten, övervaka och styr vad användarna gör och säkerställ lämpliga behörigheter i appar.
4. Övervakas laster och utfärdas varningar i samband med avvikande beteende?	☐ Övergå från dataskydd i nätverkets utkant till datadrivet skydd.
5. Använder ni maskininlärningsbaserat skydd mot hot och filtrering med sammanhangsbaserade signaler?	☐ Använd telemetri för att identifiera angrepp och anomalier, blockera och flagga riskabelt beteende automatiskt.

Kom i gång med de här resurserna:

- Testa bedömningsverktyget Noll förtroende.
- Få tio tips på hur du kommer igång med Noll förtroende.
- Lär dig hur du inför Noll förtroende i hela organisationen.

Skydda mot nätfiske och avancerade hot

Skydda organisationen mot sofistikerade hot som nätfiske och helt nya skadliga program på olika domäner.

Användbara frågeställningar	Rekommenderade aktiviteter
1. Har ni inbyggda säkerhetsfunktioner i e-posttjänsten?	☐ Aktivera säkerhetsfunktionerna i e-posttjänsten.
2. Har ni en effektiv autentiseringslösning?	☐ Använd Microsoft Azures multifaktorautentisering på alla konton för att höja säkerheten.
3. Vet du hur du känner igen nätfiskeangrepp?	☐ Utbilda dig själv, dina vänner och kollegor om hur man känner igen nätfiskeförsök och rapporterar misstänkta företeelser.
4. Är lösningen för skydd av slutpunkter komplett och automatiserad?	☐ Använd Microsoft Defender Advanced Threat Protection till förebyggande skydd av slutpunkter, upptäckt efter intrång, automatiserad undersökning och respons.
5. Har ni en integrerad lösning för skydd mot hot som kan användas för att visa samtliga hot i en centraliserad vy?	☐ Analysera hotdata från alla domäner och få en helhetsbild av varje angrepp på en enda instrumentpanel med Microsoft Threat Protection.

Kom i gång med de här resurserna:

- Hämta e-boken Office 365 Advanced Threat Protection.
- Få en modern plan för slutpunktsskydd.
- Se hur ett integrerat skydd mot hot kan höja säkerheten.

Skydda känslig information

Behovet av att skydda och styra data och hantera risker är avgörande för digitaliseringen.

Användbara frågeställningar	Rekommenderade aktiviteter
1. Vet du var era affärskritiska och känsliga data finns och vad som görs med dem?	☐ Använd flexibla och intelligenta klassificeringsfunktioner för att få hjälp att identifiera känsliga data.
2. Hur skyddar du data konsekvent i hela den digitala egendomen – utan att påverka slutanvändarnas produktivitet?	☐ Skydda data i hela hybridmiljön med en enhetlig administratörskonsol.
3. Har du kontroll över data som rör sig inom och utanför organisationen?	☐ Kontrollera åtkomsten för ohanterade enheter och välj om de ska ges fullständig åtkomst, enbart webbaserad åtkomst eller ingen åtkomst alls.
4. Använder ni flera lösningar för att klassificera, märka och skydda data?	☐ Utöka lösningen till appar och tjänster från tredje part för att skapa en bokstavligen heltäckande dataskyddslösning.

Kom i gång med de här resurserna:

- Få en översikt över Microsoft Information Protection and Governance.
- Lär dig mer om Microsoft Information Protection-meddelanden.
- Läs e-boken Metodtips för dataskydd.

Motverka interna risker

Identifiera snabbt och vidta åtgärder mot allvarliga, interna risker och åtgärda överträdelser av företagets uppförandekod i företagets kommunikation.

Användbara frågeställningar	Rekommenderade aktiviteter
1. Hur sårbar är organisationen för insiderhot?	☐ Ta fram en policy för att hantera insiderrisker och tilldela åtkomster för hantering av insiderrisker och granskningsloggen.
2. Hur kan du hjälpa till att skydda företaget mot potentiella insiderrisker?	☐ Granska och övervaka potentiella risker inklusive stöld av personaluppgifter, dataläckor och stötande språkbruk på en instrumentpanel med varningar.
3. Kan ni skyndsamt upptäcka överträdelser av uppförandekoden i företagets kommunikation?	☐ Anpassningsbara mallar för policyefterlevnad i kommunikation kan användas för att upptäcka och åtgärda överträdelser av uppförandekoden.
4. Uppfyller företagets kommunikation gällande regelverk och kravet på tillsyn?	☐ Ta fram en policy för att säkerställa att kommunikation följer regelverket när det gäller etik, företagsstandarder, lagar och regler.

Kom i gång med de här resurserna:

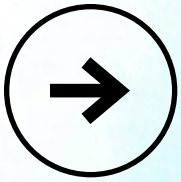
- Ta reda på hur ni kan använda AI och maskininlärning för att hantera insiderrisker.
- Kom igång med hantering av insiderrisker.
- Håll dig uppdaterad med vår Insider Risk-blogg.

Bygga upp motståndskraft genom att förbättra cybersäkerheten

Motståndskraft i driften kan inte uppnås utan att man verkligen satsar på och investerar i motståndskraft mot cyberhot. Globala organisationer behöver uppnå ett tillstånd där deras kärnverksamhet och tjänster inte störs av geopolitiska eller samhällsekonomiska händelser, naturkatastrofer eller cyberhändelser, om de ska kunna rida ut sådana händelser och behålla sin styrka.

Microsoft Security-lösningar kan lägga grunden till motståndskraft mot cyberhot genom att tillhandahålla en smidig användarupplevelse tillsammans med förstklassigt, integrerat skydd.

Om du vill veta mer om hur Microsoft Security kan stärka din organisation finns våra säljrådgivare här för att hjälpa dig.



Kontakta oss