Cybersäkerhetsrisker

I dagens digitala värld står både företag och privatpersoner inför ständiga hot från cyberattacker. Vanliga risker inkluderar malware (skadlig programvara), phishing (falska e-postmeddelanden för att stjäla information), dataintrång, och DDoS-attacker (överbelastningsangrepp som slår ut tjänster). Dessa hot kan leda till ekonomiska förluster, skada varumärkets rykte och förlust av känslig information.

Nedan följer en checklista du kan använda för att påbörja ditt Cybersäkerhetsarbete.

Checklista för Cybersäkerhet

1. **Starka Lösenord och Autentisering**
    - Använd långa, komplexa lösenord (minst 12 tecken).
    - Aktivera tvåfaktorsautentisering (2FA) där det är möjligt.
    - Använd en lösenordshanterare för att lagra och skapa säkra lösenord.
2. **Säkerhetsuppdateringar och Patchar**
    - Installera omedelbart säkerhetsuppdateringar för operativsystem och programvara.
    - Använd automatisk uppdatering om möjligt.
3. **Brandväggar och Antivirus**
    - Aktivera en brandvägg för att skydda nätverket.
    - Installera och uppdatera antivirusprogram regelbundet.
    - Gör regelbundna säkerhetsskanningar.
4. **Säkerhetskopiering**
    - Gör regelbundna säkerhetskopior av viktig data, helst till en extern plats eller molnet.
    - Testa återställningsprocedurer för att säkerställa att säkerhetskopiorna fungerar.
5. **E-postsäkerhet**
    - Var vaksam mot phishing-mejl och klicka inte på misstänkta länkar eller bilagor.
    - Bekräfta avsändarens identitet innan du delar känslig information.
6. **Åtkomstkontroll**
    - Begränsa användares åtkomst till data och system baserat på deras arbetsuppgifter (principen om minsta privilegium).
    - Använd roller och grupper för att hantera åtkomst rättigheter.

Qnetworks AB, Frykdalsbacken 12, plan 3. 123 43 Farsta. Tel: 08-10 10 90
www.qnetworks.se | info@qnetworks.se

7. **Säkerhet för Mobila Enheter**
    - Använd lösenord eller biometrisk autentisering på alla mobila enheter.
    - Aktivera fjärrradering för att skydda information om enheten försvinner.
8. **Kryptering**
    - Kryptera känsliga data både i vila (på hårddiskar) och under överföring (när det skickas över nätverket).
9. **Säkerhetsmedvetenhet**
    - Utbilda medarbetare regelbundet om cyberhot, phishing och social ingenjörskonst.
    - Uppdatera policyer och riktlinjer för cybersäkerhet i organisationen.
10. **Incidenthanteringsplan**

- Utveckla en plan för hur ni ska hantera säkerhetsincidenter.
- Öva på planen regelbundet för att säkerställa att alla vet vad de ska göra vid en attack.

11. **Övervakning och Loggning**

- Implementera övervakning av nätverk och system för att upptäcka misstänkt aktivitet.
- Spara och granska loggfiler för att identifiera och svara på incidenter.

12. **Användning av VPN**

- Använd VPN (Virtual Private Network) när du ansluter till offentliga eller osäkra nätverk för att kryptera internettrafiken.

Denna checklista täcker viktiga steg för att stärka cybersäkerheten och minska risken för attacker och intrång.

Tveka inte att kontakta oss eller kolla in vår hemsida för mer info.

info@qnetworks.se

www.qnetworks.se/utbildning/cyber

Qnetworks AB, Frykdalsbacken 12, plan 3. 123 43 Farsta. Tel: 08-10 10 90
www.qnetworks.se | info@qnetworks.se