CYBERLY

In our open and connected world, opportunities are endless. Yet, in the face of continuous technology development, so are the vulnerabilities. We want to embrace continuous change and at the same time enhance everyone's digital resilience to help create a safe, sustainable, and efficient society.

We call our ecosystem Cyberly

We are a well-connected cluster of members and a vibrant network of stakeholders, where we build trust to share insights and experience with each other and spread the knowledge around digital resilience.

Our approach is ACT Cyberly, which calls for conscious action. Staying ahead and ensuring that securing digital assets and systems are managed along with overall security of an organisation and as part of reaching its overall goals.

Our starting point is the region of Östergötland, Sweden, well-known for its industrial and military heritage, defence and security industry and deep tech startups, scaleups and grownups.

We are one of four clusters in Linköping Science Park – the home of groundbreaking innovations and one of Sweden's largest and oldest science parks. For 40 years, innovations, entrepreneurs, and new companies have started, grown, and developed the world with Linköping as their base.

Our Science Park is a world-class innovation hotspot – with leading tech companies such as Sectra, Actia and Magna, as well as pioneering startups like Epishine, Polar Lights and Nano Textiles. It is a place where businesses grow and break frontiers in close collaboration with academia and talents.

ACT cyberly

STÄRK DIN DIGITALA RESILIENS

HANDFASTA TIPS: CYBERHYGIEN

PROAKTIVITET OCH INFRASTRUKTUR

Region Östergötland

Medfinansieras av Europeiska unionen

MED FINANSIERING FRÅN tillväxtverket

Cyberhygien – dina första steg till en säkrare digital vardag

- **Skapa starka och unika lösenord till dina olika konton**
- **Spara dina lösenord i en lösenordshanterare**
- **Aktivera 2-faktorsautentisering på alla konton där det är möjligt**
- **Håll alltid enheter uppdaterade**
- **Säkerhetskopiera viktig data**
- **Skärmsläckare på alla enheter**
- **Begränsad access och rättigheter för medarbetare**
- **Flyttta inte arbetsrelaterade samtal till privata kanaler**
- **Använd krypterade appar, t ex Signal**

Digital infrastruktur – vår resiliens börjar lokalt

Säkra din egen styrka genom att koppla din omnejd till andra närliggande omnejder och skapa redundans. Men också genom att tänka över vilka beroendeförhållanden du går in i. Några tips avseende digital infrastruktur är:

- **Fastställ organisationens huvuduppgifter och vilka som är absolut viktigast.**
  - Tänk hela verksamheten, inte bara IT eller specifika tjänster ni omsätter mycket på.
  - Utgå från regleringsbrev, förordning, eller ägardirektiv.
- **Identifiera dina beroenden med fokus på det som behövs för att det ni har kommit fram till är viktigt ska fungera oavsett vad, även över tid.**
  - Vilka av dessa beroenden hanterar ni själva och vilka är ni beroende av tredje part för att kontrollera?
  - Vilka beroenden kan ni ersätta? Exempelvis: går det att ersätta journalsystemet med papper och penna om så krävs, eller finns det någon som kan göra personalplanering för månaden om all elektronisk personalplanering försvinner?
- **Identifiera beroenden som ni inte kan ersätta.**
  - Där det går, bygg teknisk diversitet, där tjänster kan ersätta varandra om en slutar att fungera. Lägg inte alla ägg i en korg.
  - Köp tjänster och produkter med kända beroenden, för att motverka allt från dubbelförläggning till andra gemensamma beroenden.
- **Prata med dina grannar och vänner – partnerorganisationer och nätverk.**
  - Öva tillsammans på att lösa ut det som är viktigt så att ni vet hur ni ska agera, och att det verkligen fungerar att agera så.

Identifiera kritisk information

För ett register över viktiga uppgifter, såsom kontaktuppgifter, epost, kalendrar och andra väsentliga dokument. Identifiera vilka nyckelsystem och resurser som krävs för att verksamheten ska fungera. Att ha resonerat om systemen och informationen är halva arbetet. Det väcker en förståelse för vad som kan hända om informationen blir otillgänglig eller kommer på villovägar.

Identifiera dina viktigaste partners

Gör en förteckning över dina viktigaste partners. Detta underlättar ditt agerande i händelse av en incident och gör det möjligt för dig att hålla din organisation aktiv i händelse av otillgängliga system. Se t.ex. till att ha kontaktnummer för leverantörer, nummer för IT-support osv. Detta bör vara lagrat på en plats du kommer åt även om det inte går att logga in på företagets egna system eller molntjänster.

Säkerhetskopiera regelbundet

Testa att säkerhetskopian fungerar för att se till att du kan återställa informationen då det behövs. Enklast är att göra stickprov på viktiga dokument. Är det backup i molnet? Är det något som inte backas upp dit som du behöver hantera själv? Och klarar leverantören att hantera återställning om ni drabbas av utpressningvirus som låser alla filerna?

Gör en incidentplan

Förvara din incidentplan på ett säkert sätt så att du kan använda den om din utrustning stjäls eller skadas av en cyberincident. Med andra ord är det bra om den finns tillgänglig även i fysisk form. Finns några intressenter som behöver information omgående? Behöver du rapportera om läckta personuppgifter (GDPR) till Integritetsmyndigheten? Vilka manuella steg kan du använda i stället för vad du vanligen gör digitalt i olika system?

Lösenordshanterare

Varför?

En lösenordshanterare gör det möjligt att ha långa, komplexa och enskilda lösenord till olika konton utan att du behöver ha dem memorerade i huvudet.

Fokusera först och främst på organisationskritiska konton. Detta är viktigt eftersom du annars riskerar att ett enda lösenord på vift kan ge angripare tillgång även till andra inloggningar.

Hur?

Det finns många lösenordshanterare att välja bland, vissa bättre än andra. En vi rekommenderar som ett säkert alternativ är Bitwarden. Du kommer långt på gratisvarianten. Du kan installera den både på din dator och mobil, vilket gör att du kan spara ditt lösenord på ena enheten och sedan sömlöst använda den på den andra.

Bitwarden

Starka lösenord är egendomliga fraser

- **Exempel på starkt lösenord: *“Bertil kör alltid 4 elefanter.”***
- **Lätt att komma ihåg och svårt att knäcka!**
- **Svaga lösenord kan hackas på nolltid!**
- **Grundregeln är att längden är viktigare än komplexiteten. Bilda därför gärna en mening av udda sammansatta ord enligt ovan.**

2-faktorsautentisering (2FA)

Varför?

2FA ger dig ett extra skydd så att cyberbrottslingar inte kan komma åt ditt konto även om de skulle komma över ditt lösenord. Om du kräver 2FA, så måste någon ha tillgång till två av dina eneter för att ta sig in och det är svårare än att bara ha den ena. 2FA fungerar genom att be om ytterligare information för att bevisa din identitet. Du får till exempel en kod skickad till din telefon när du loggar in med en ny enhet eller ändrar inställningar som till exempel ditt lösenord.

Hur?

Börja med att aktivera 2FA (också kallat MFA) för din epost och gör det sedan för alla dina viktiga konton och system som har stöd för det. Som regel får du logga in på din molntjänst och gå till inställningar för att aktivera det och där följa instruktionerna. Som regel så kräver det en applikation som du har installerad på din dator eller telefon, så som exempelvis Microsoft Authenticator om du kör Microsoft Windows eller inbyggda Keychain om du kör Apples produkter.

Håll dina enheter uppdaterade

Se alltid till att alla enheter har de senaste uppdateringarna för att minska risken för cyberincidenter. På så sätt minskar du risken för att någon angripare utnyttjar olika hål som kan finnas. Se alltid till att uppdatera på förfrågan. Var dock säker på att förfrågan kommer från rätt håll och att ingen försöker lura dig med popup-fönster på en hemsida till exempel.

Säkerhetskopiera viktig data

Det är lätt att förstå varför man vill vara försäkrad efter att huset brunnit ned. Säkerhetskopiering är en försäkring som gör att din organisation fortsätta att fungera även om du drabbas av en cyberincident. Säkerhetskopiorna kan innefatta papperskopior, flyttbara medier eller säkerhetskopior till molnet.

Proaktivitet – förbered dig för en cyberincident

Även om det är viktigt att införa bra säkerhetskontroller finns det ingen perfekt säkerhet, då hotbilden ständigt förändras.

Alla organisationer löper risk att drabbas av en potentiell cyberincident, så det är viktigt att du förbereder hur du kan svara på det och planerar återställning i händelse av att det skulle hända.

- **Identifiera kritisk information**
- **Gör en förteckning över dina viktigaste partners som du använder för att driva din organisation**
- **Säkerhetskopiera regelbundet viktig information**
- **Gör en sårbarhetsanalys**
- **Upprätta incidentplan**
- **Öka förståelse att varje medarbetare är en del av säkerheten och våga ställa krav**
- **Det ska vara lätt att göra rätt**
- **Uppmuntra till att erkänna misstag och dela lärdomar**