IT-Säkerhet
steg för steg

En svensk IT- och säkerhetspartner med
egen drift och support i Stockholm.

www.fiberdirekt.se

Regelverket skärps, vi gör efterlevnaden enkel

Cybersäkerhetslagen, Sveriges genomförande av EU:s NIS2-direktiv, har trätt i kraft och omfattar fler verksamheter än tidigare. För många är ett ledningssystem som ISO 27001 nästa naturliga steg. Samtidigt är hoten vardag, inte rubriker. Det handlar sällan om avancerade angripare, oftare om en gammal inloggning eller en behörighet ingen hann ta bort.

NIS2

Fler sektorer omfattas, med krav på riskhantering, incidentrapportering och ett tydligt ledningsansvar.

8 av 10

incidenter börjar i en identitet, ett lösenord eller en behörighet, inte i ett raffinerat intrång.

Ansvaret

ligger numera hos ledningen, inte enbart hos IT. Det går inte att delegera bort.

Det farligaste i er IT är oftast det enklaste ni inte hunnit med.

Svenskt huvudmannaskap, snabb lokal service

Vi är en svensk IT- och säkerhetspartner som finns nära er verksamhet. Med fiber, datacenter, drift och säkerhet i egen regi får ni en partner med tydligt ansvar, korta beslutsvägar och personer ni kan prata direkt med. Det är tryggheten i att välja en lokal aktör framför en stor internationell leverantör, där supporten ofta är anonym, ansvaret uppdelat och driften långt från er vardag.

Svenskt huvudmannaskap

Svenskt ägande och svensk drift. Er data lagras och driftas i Sverige, under svensk lag och utanför räckvidden för internationell lagstiftning som till exempel Cloud Act.

ISO 27001 och 14001

Inte bara dokumentation, utan ett arbetssätt som genomsyrar vardagen.

En partner som känner er

Samma team över tid. Människor som lär känna er miljö och svarar snabbt när ni ringer, under 10 sekunder i genomsnitt under 2025.

Vi tar ansvar för hela kedjan

Från fiber och datacenter till drift och säkerhet. Ni får en partner som håller ihop helheten, så att ansvar inte faller mellan olika leverantörer.

Er data stannar i Sverige, hos en partner ni faktiskt kan ringa.

Grunden för ett förebyggande skydd

Ett beprövat arbetssätt, anpassat efter er verksamhet. Vi utgår från NIST CSF 2.0: styra, identifiera, skydda, upptäcka, hantera och återställa, men gör det praktiskt och relevant för er miljö. Här visar vi var Fiber Direkt går in, och vad vi prioriterar först för att bygga en säker och förebyggande grund.

- **Börja resan mot ett tryggare och mer hållbart skydd**

1 Styra

- Roller och ansvar
- Policy, ledningsuppföljning

2 Identifiera

- Kartläggning
- EASM, extern exponering

3 Skydda

- MFA och Keycloak SSO
- Segmentering

4 Upptäcka

- Övervakning
- Domänbevakning

5 Hantera

- Incidenthantering

6 Återställa

- Backup och drift

Mindre angreppsyta börjar med rätt åtkomst

Vi börjar där effekten är störst: era identiteter. De flesta angrepp tar sig in genom en inloggning, inte genom en brandvägg.

1 Identitet och IAM

Ordning på vem som får vad. Vi rensar gamla konton och samlar inloggningen på ett ställe.

2 RBAC, roller

Behörighet efter roll, inte efter vana. Var och en kommer åt precis det jobbet kräver.

3 Keycloak SSO

En inloggning till allt, på en öppen plattform ni äger själva. Färre lösenord, full kontroll.

4 MFA med YubiKey

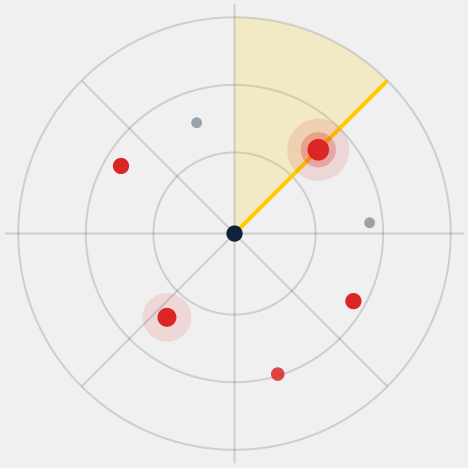
Inloggning som kräver mer än ett lösenord. En fysisk nyckel (YubiKey) stoppar nätfiske i praktiken helt.

Identiteter styr vem som kommer åt vad. Därför börjar vi där.

Vet ni vad som syns utåt?

EASM, External Attack Surface Management, handlar om att kartlägga det som går att nå från internet. Det visar era domäner, system, tjänster och exponeringar, både det ni känner till och det som kan ha glömts bort. När vi vet vad som syns kan vi minska ytan, stänga onödiga vägar in och åtgärda risker innan någon annan hittar dem.

- **Domäner och webbplatser**
  Även gamla kampanjsajter ingen mindes.
- **IP-adresser och öppna portar**
  Vad som faktiskt går att nå utifrån.
- **Exponerade maskiner och tjänster**
  Servrar och system som står öppna.
- **Läckta uppgifter och certifikat**
  Lösenord på vift, certifikat som löpt ut.



Vill ni gå djupare kan vi göra ett avgränsat **pentest på begäran**. Då tar vi oss faktiskt in, under kontrollerade former, och visar exakt vad som behöver åtgärdas.

Tjänster på kran

Börja där behovet är störst och lägg till mer när det passar. Våra säkerhetstjänster kan skalas steg för steg, utan inlåsning och med öppna standarder som gör att valet alltid är ert.

Kartläggning
Nuläge och prioriteringar.

EASM
Bevakning av er angreppsyta.

MFA och IAM
Identitet och stark inloggning.

Keycloak SSO
En inloggning till allt, ni äger den.

Segmentering
Dela nätet, begränsa skadan.

Sårbarhetsbevakning
Löpande skanning, larm vid avvikelse.

Incident och backup
Hantera och återställ snabbt.

Manuellt pentest
Avgränsat, vi testar på riktigt.

Virtuell CISO
Rådgivning och praktisk hjälp.

- Ingen inlåsning ✓
- Öppna standarder ✓
- Skala upp och ner ✓
- Svensk drift ✓

Svensk trygghet genom alla lager

Från fiber och datacenter till drift och säkerhet bygger vi på en svensk, certifierad och redundant kedja. Det ger säkerhetsarbetet en stabil grund att stå på.

Hosting i Sverige

System och data i svenska datahallar. Under svensk lag.

Skalbar kapacitet

Växa utan att binda kapital i egen hårdvara.

Byggt för avbrott

Dubbla vägar, reservkraft och hög tillgänglighet.

ISO-certifierad grund

27001 och 14001 genom hela infrastrukturen.

Svensk och europeisk grund

Ägande, drift och data i Sverige, under svensk och europeisk lagstiftning. En tydlig grund för kontroll, regelefterlevnad och minskad exponering mot utomeuropeisk lagstiftning.

Ett säkerhetsteam, på era villkor

TVÅ ROLLER

Virtuell CISO, deltid och löpande. Eller **interim CISO** vid omställning, på offert.

TVÅ UPPLÄGG

Retainer, löpande och förutsägbart. Eller **projekt**, avgränsat med fast pris.

TVÅ SÄTT ATT KÖPA

Lös timme, 1 495 kr. Eller **abonnemang** från 1 166 kr/tim med mängdrabatt.

vCISO Bas

5 %

5 timmar i månaden

6 151 kr /mån

1 230 kr/tim

Löpande rådgivning och stöd i enskilda frågor.

vCISO Plus

Populär

10 timmar i månaden

11 914 kr /mån

1 191 kr/tim, 8 % rabatt

Aktivt arbete med regelefterlevnad, risk och säkerhetsutveckling.

vCISO Premium

10 %

20 timmar i månaden

23 310 kr /mån

1 166 kr/tim

Höga krav på styrning, rapportering och NIS2-anpassning.

- **Betydligt billigare än en anställd CISO, men med tillgång till ett helt säkerhetsteam.**

Alla priser exklusive moms.

Tilläggstjänster som stärker skyddet

Det här ingår i vCISO

- Strategisk rådgivning inom informations- och cybersäkerhet
- Risk- och sårbarhetsanalyser
- Stöd för NIS2, GDPR och ISO 27001
- Policyer och styrdokument
- Rapportering till ledningsgrupp
- Leverantörs- och tredjepartsgranskning
- Incidenthantering och kontinuitetsplanering
- Säkerhetsutbildning och ledningsstöd
- Samordning av EASM, pentest och revision

Kontinuerlig sårbarhetsbevakning

Bas: automatiserade skanningar och rapporter	**990 kr/mån**
Plus: kurerad och tolkad av er vCISO	**1 500 till 3 000 kr/mån**

Manuellt penetrationstest

Avgränsat engångsuppdrag där vi testar på riktigt.

På begäran, från ca 30 000 kr

Workshop: MFA, YubiKey och LastPass

Utbildning och installation i grupp om 5 personer, ca 6 timmar.

20 000 kr per tillfälle

Migrering av befintlig IT-miljö

Vi planerar migreringen steg för steg tillsammans med er. Lösningen anpassas efter hur ni vill arbeta framåt, helt hos oss, i en hybridmodell eller med delar kvar i er egen miljö.

TILLÄGGSTJÄNSTER, PÅ OFFERT

Säkerhetsrevision · NIS2-gap-analys · Utökad EASM · SOC och SIEM-övervakning · Incidentövningar och krisledning · IEC 62443 och OT-säkerhet

Alla priser exklusive moms. Resor och eventuella omkostnader debiteras separat.

Ni väljer budgetnivå. Vi hjälper er prioritera rätt

Så här kan det se ut för ett medelstort företag som börjar från noll. Plocka bort eller lägg till, summan följer med. Det här är ett exempel, inte en offert.

LÖPANDE, PER MÅNAD

vCISO Plus, 10 tim i månaden	**11 914 kr**
Sårbarhetsbevakning, Plus	**2 500 kr**
Summa löpande	**14 414 kr** /mån

ENGÅNG, VID UPPSTART

MFA-workshop, grupp om 5 personer	**20 000 kr**
YubiKey-nycklar, 5 personer × 2 st	**5 500 kr**
Manuellt penetrationstest	**från 30 000 kr**
Migrering av IT-miljö	**på offert**
Summa engång	**från 55 500 kr**

UNGEFÄR FÖRSTA ÅRET

≈ 230 000 kr

Löpande stöd i tolv månader plus uppstart. Därefter bara den löpande månadskostnaden. Skala upp eller ner när som helst.

Illustrativt räkneexempel, alla priser exklusive moms. Faktisk kostnad beror på omfattning och vilka komponenter ni väljer.

Börja med det som ger mest, snabbast

Börja där det gör mest nytta. Välj ett eller flera första steg som ger snabb effekt, så hjälper vi er att bygga vidare i rätt takt.

1. **Aktivera MFA med YubiKey**
   Skydda konton med fysisk nyckel och ge teamet en enkel, säkrare inloggning.

2. **Sätt upp ett manuellt pentest på begäran**
   Se svart på vitt var ni står, och vad som behöver lagas först.

3. **Samla inloggningen med Keycloak SSO**
   En säker inloggning till era system. Färre lösenord, tydligare behörigheter och bättre kontroll över vem som kommer åt vad.

4. **Virtualisera era fysiska servrar i Sverige**
   Flytta från lokal hårdvara till svensk virtualisering med bättre kontroll, redundans och skalbarhet.

Det här är hela bilden

En sida att ta med till ledningsgruppen.

Risken	De flesta angrepp börjar i en identitet eller något enkelt ingen hann med. Det farligaste är sällan det mest avancerade.
Regelkraven	Cybersäkerhetslagen (NIS2) ställer krav på riskhantering, rapportering och ett ledningsansvar som inte går att delegera bort. ISO 27001 är ofta nästa steg.
Vägen	Förstå verksamheten, säkra identiteterna (MFA och SSO), få koll på angreppsytan, och bygg vidare i er takt längs NIST-kartan.
Investeringen	Löpande stöd via virtuell CISO från 6 151 kr/mån. Kontinuerlig sårbarhetsbevakning från 990 kr/mån. MFA-workshop 20 000 kr per tillfälle. Skala i er takt, alla priser exklusive moms.
Varför oss	Svensk kontroll, certifierad grund och ett ansvar som håller ihop. Vi bygger säkerhet på infrastruktur ni kan lita på, utan inlåsning och utan att tappa helheten.

Orden, i klarspråk

Vi vet att förkortningar kan bli onödigt svåra. Därför har vi samlat dem här, på vanlig svenska.

NIS2 *lagkrav*
Network and Information Security Directive 2
EU-direktiv, infört i svensk lag som Cybersäkerhetslagen, med krav på säkerhetsarbete och rapportering.

ISMS *förk.*
Information Security Management System
Ledningssystem för informationssäkerhet, ett strukturerat sätt att styra säkerheten.

ISO 27001 *standard*
Ledningssystem för informationssäkerhet
Internationell standard och certifiering för ett sådant ledningssystem.

MFA *förk.*
Multi-Factor Authentication
Flerfaktorsautentisering, inloggning som kräver mer än bara ett lösenord.

SSO *förk.*
Single Sign-On
En inloggning som ger åtkomst till flera system.

RBAC *förk.*
Role-Based Access Control
Rollbaserad behörighet, åtkomst styrs av roll, inte av person.

PAM *förk.*
Privileged Access Management
Hantering av privilegierade konton, extra skydd för de mäktigaste behörigheterna.

EASM *förk.*
External Attack Surface Management
Kartläggning av allt i er IT som syns och går att nå från utsidan.

Pentest *metod*
Penetrationstest
Kontrollerat intrångstest, vi försöker ta oss in för att hitta hålen först.

vCISO *förk.*
Virtual Chief Information Security Officer
Virtuell säkerhetschef, en CISO på deltid, löpande eller per uppdrag.

CIA-triaden *begrepp*
Confidentiality, Integrity, Availability
Konfidentialitet, riktighet och tillgänglighet, säkerhetens tre grundfrågor.

NIST CSF *ramverk*
NIST Cybersecurity Framework
Etablerat ramverk som delar säkerhetsarbetet i sex tydliga funktioner.

Slå oss en signal, så tar vi det därifrån

KONTAKT

team@fiberdirekt.se

08-510 615 70

www.fiberdirekt.se

ADRESS

Odengatan 28, Stockholm

Mailbox 392, 111 73 Stockholm