TELE2

Guiden till ett tryggt och motståndskraftigt företag

Cyberattacker och dataintrång illustreras ofta med en ensam person i mörk huvtröja som hackar sig in i datorer och system, men det är sällan så det går till.

I stället sker attacken vanligtvis genom helt vardagliga händelser. Kanske kommer intrånget i ett mejl som ser ut att vara från en samarbetspartner, eller genom att ett lösenord återanvänds på fel ställe.

Sedan kan det gå fort. Plötsligt är företagets filer krypterade mot lösensumma, kunddatabasen ligger ute till högstbjudande på darknet, och era webbplatser och appar är nere för räkning. Detta är tyvärr inga skräckscenarier, utan tre av de vanligaste attackerna mot svenska företag.

Det är inte bara större företag som drabbas. Cyberattacker är opportunistiska och går ut på att utnyttja verksamhetens svagheter, oavsett i vilken organisation de uppstår. Skillnaden är marginalerna. En attack som "bara" orsakar allvarliga problem för ett stort företag kan slå undan benen helt för ett mindre.

Den goda nyheten är att några av de viktigaste skydden inte kostar något. Det handlar inte om fysiska produkter och licenser, utan om medvetenhet och vanor – som att slå på flerfaktorautentisering och aldrig återanvända lösenord.

I den här guiden tittar vi närmare på hur konkreta risker kan se ut, vilka åtgärder som gör mest nytta, och hur ni bygger säkerhet som skyddar verksamheten utan att bromsa den.

TELE2

Följ en attack – och stoppa den

Cyberattacker varierar stort i allvarlighetsgrad och konsekvenser, men de flesta följer samma övergripande mönster: angriparen exploaterar en svaghet, tar sig in i systemen, och utnyttjar sedan åtkomsten i brottsligt syfte.

Inget av de fyra händelseförloppen till höger har ett rent tekniskt svar. I vart och ett står även en människa som antingen reagerar i tid eller inte. Det är den delen som avgör mest och den som kostar minst.

Stark säkerhet bygger på beredskap för alla delar av händelseförloppet.

1. **Hur kommer angriparen in?**
2. **Hur långt kommer angriparen när de väl är inne?**
3. **När märker ni att något är fel?**
4. **Hur snabbt kommer ni igång med verksamheten igen?**

1. Hur kommer angriparen in?

Många angrepp börjar på ett av två sätt: inloggningsuppgifter hamnar i fel händer, eller någon luras att öppna dörren och släppa in angriparen via exempelvis nätfiske.

Starka lösenord är viktiga men inte tillräckliga, eftersom de ibland läcker och sällan ändras. Flerfaktorsautentisering (MFA eller *Multi Factor Auhentication*) via till exempel app eller sms är en enkel och effektiv åtgärd som ökar säkerheten markant. Det krävs då mer än ett läckt lösenord för att angriparen ska ta sig in.

I de flesta mejl- och molntjänster ingår denna funktionalitet som standard, men är inte nödvändigtvis aktiverad. Generellt ser vi att MFA används mest inom offentlig sektor och större företag, och användningen har ökat under senare år när distansarbete blivit vanligare. Men flerfaktorautentisering används idag endast av 50-60 procent av företag och organisationer i Skandinavien, så här finns fortfarande stora möjligheter till förbättring.

Den andra vägen in – att en medarbetare luras att släppa in angriparen – är svårare att stänga, eftersom den går via människor. Nätfisket blir mer avancerat för varje år, inte minst tack vare ai, och avsändare går att förfalska.

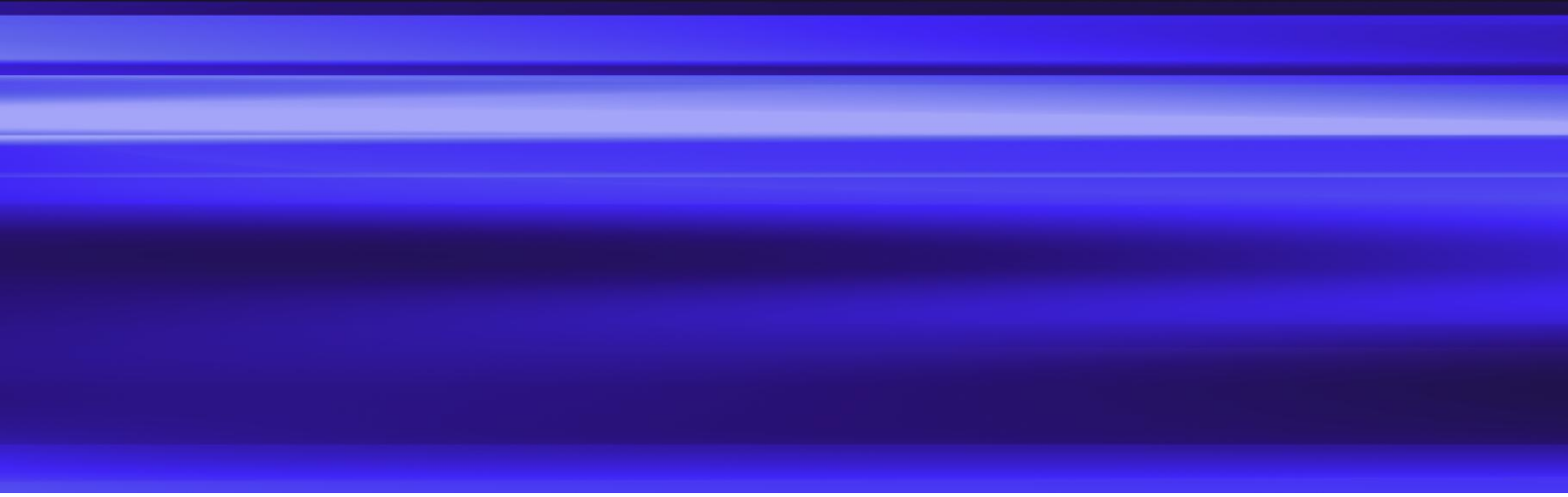
> "En angripare kan göra hundratals mejlutskick utan att själv behöva vara aktiv. Hackaren behöver bara förbereda en distributionslista som mejlen ska gå ut till och sedan luta sig tillbaka och vänta på att någon råkar göra fel."
>
> **Torbjörn Zars**
> Säkerhetsexpert på Tele2 Företag

Tre enkla åtgärder med stor effekt

- Slå på flerfaktorsautentisering överallt där det går, med start på mejlen.
- Sätt automatiska uppdateringar på datorer, mobiler och servrar, så att de inte är beroende av den enskilda medarbetaren för att bli utförda.
- Använd lösenordshanterare, så att inget lösenord återanvänds mellan tjänster.

Lösningar från Tele2

Autentisering och flerfaktorsautentisering, Auto Enrollment för automatiserad användarregistrering, samt mejlskydd som stoppar nätfiske och skadlig kod innan det når fram.



2. Hur långt kommer angriparen när de väl är inne?

Att obehöriga tar sig in i företagets system är illa nog. Om de sedan kan röra sig fritt är det avsevärt värre. Skillnaden och allvarlighetsgraden avgörs av hur mycket varje enskild inloggning eller enhet faktiskt ger tillgång till.

Behörigheter är en grundläggande faktor. Alla medarbetare behöver inte ha tillgång till allt. Konton som tillhör medarbetare som slutat, eller rättigheter som inte används, är dörrar som står på glänt utan att någon märker det.

Att städa bland behörigheterna är ofta enkelt, men att hålla ordning på längre sikt kan vara en större utmaning. När systemen blir fler och medarbetare byter roller kan behörigheterna snabbt växa bortom överblick. I det läget är det värt att låta behörigheten följa rollen i stället för personen, så att både registrering och avregistrering sker av sig självt om en medarbetare slutar eller byter roll på företaget.

Sedan har vi enheterna. När mobiler och bärbara datorer kommer på avvägar är den viktigaste frågan inte vad den förlorade enheten kostade, utan vad den innehöll. Skärmlås och diskkryptering finns inbyggda i moderna datorer och mobiler, och de bör vara aktiverade utan undantag. Om verksamheten har många enheter är central hantering det som gör att en borttappad telefon kan låsas eller raderas på distans.

Då kvarstår också frågan om hur mycket nätverket själv lämnar ut.

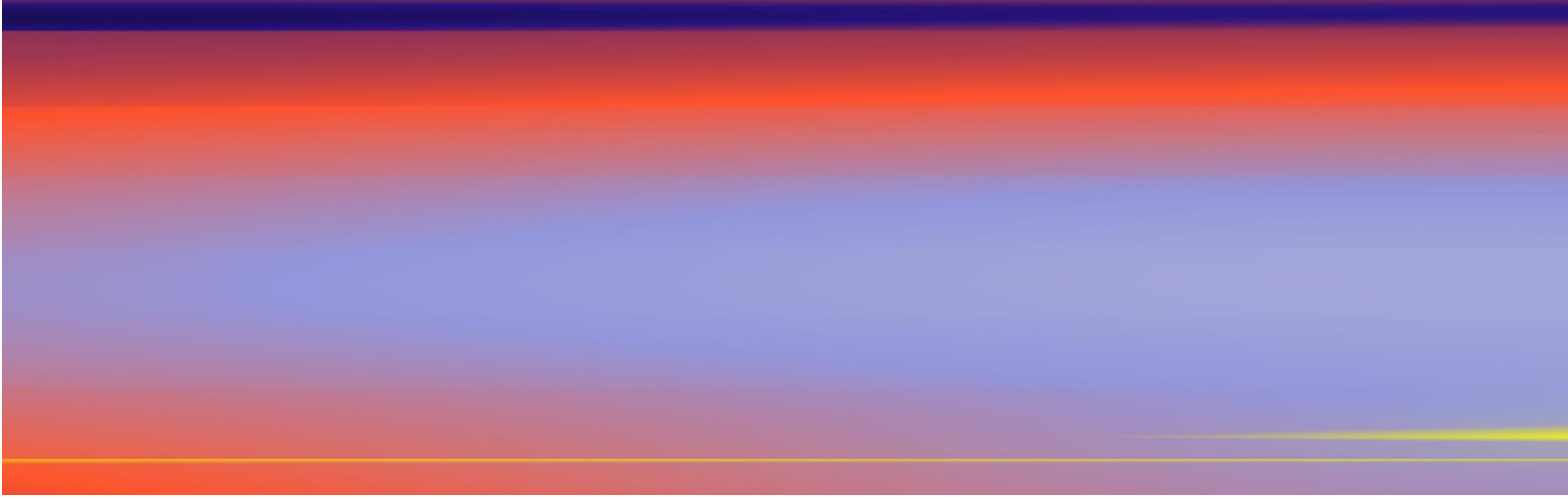
Det vanliga i mindre verksamheter är att det mesta ligger på samma nät – ekonomisystemet, filservern, skrivaren och gäst-wifi. Den som tagit sig in på ett ställe är då i praktiken inne överallt. Att dela upp nätet i zoner, så att en enhet bara når det den faktiskt behöver, hör till de mest effektiva åtgärderna. Principen kallas zero trust och innebär att man inte litar på en enhet bara för att den varit ansluten förut, utan verifierar varje gång.

> "Vi rekommenderar att organisationen segmenterar sitt nät och sätter olika skydd för olika zoner och olika typer av användning, samt tar hänsyn till var användaren befinner sig och vad personen ska kunna nå."

Vincent Vanot
Säkerhetsexpert på Tele2 Företag

Lösningar från Tele2

Unified Endpoint Management (UEM) för central hantering av datorer och mobiler, Tele2 Internet Firewall, IP VPN och Mobilt VPN för skyddad uppkoppling, samt SD-WAN för verksamheter som arbetar mycket i molnet.



3. När märker ni att något är fel?

Antalet attacker ökar snabbt, och snabbare i Sverige än i Europa i övrigt. Enligt siffror som Check Point Research publicerade i juli 2026 drabbades en genomsnittlig svensk verksamhet av 2 432 cyberattacker i veckan under juni. Det är en ökning med 40 procent på ett år, mot 22 procent för Europa som helhet.

Vissa av dem märks omedelbart. En överbelastningsattack slår ut era webbtjänster utan att någon behöver ta sig in, och tröskeln är låg för de kriminella. En DDoS-attack kan beställas för så lite som 15 euro, medan förlusterna för det drabbade företaget blir mångdubbelt större.

De farligaste angreppen är dock av motsatt sort. Ingenting slutar fungera. I stället är någon inne i systemen, läser, kopierar och väntar på rätt tillfälle, utan att det märks. Globalt tar det i genomsnitt omkring 190–200 dagar att upptäcka ett intrång, vilket är mer än tillräckligt för den angripare som redan är inne. Se till att slå på inloggningsvarningar i de system som erbjuder det.

Signaler som är värda en reaktion:

- Inloggningar vid udda tider eller från platser ni inte känner igen.
- En samarbetspartner som säger sig ha fått ett konstigt mejl från er adress.
- Filer som plötsligt inte går att öppna, eller som fått nya filändelser.
- System och tjänster som blir märkbart långsammare utan förklaring.

Vad som händer (eller inte händer) sedan är avgörande. Vem larmar man, och hur? En medarbetare som misstänker något behöver veta vem man vänder sig till – och det ska vara enkelt. Se till att slå på inloggningsvarningar i de system som erbjuder det.

På den här nivån går ofta gränsen för vad de flesta mindre och medelstora företag kan hantera på egen hand. Kontinuerlig övervakning kräver att någon är vaken när ni sover, och avvikelser bör värderas av någon som vet vad de betyder. Därför är det nästan alltid mer kostnadseffektivt att lägga ut den här typen av tjänster till en extern leverantör.

Lösningar från Tele2

Tele2 DDoS Defense i tre nivåer – Basic med generiskt skyddsfilter, Basic Plus med anpassningsbara filter, och Advanced med segmenterat skydd och kundunika tröskelvärden. Därtill övervakad drift dygnet runt, alla dagar på året.

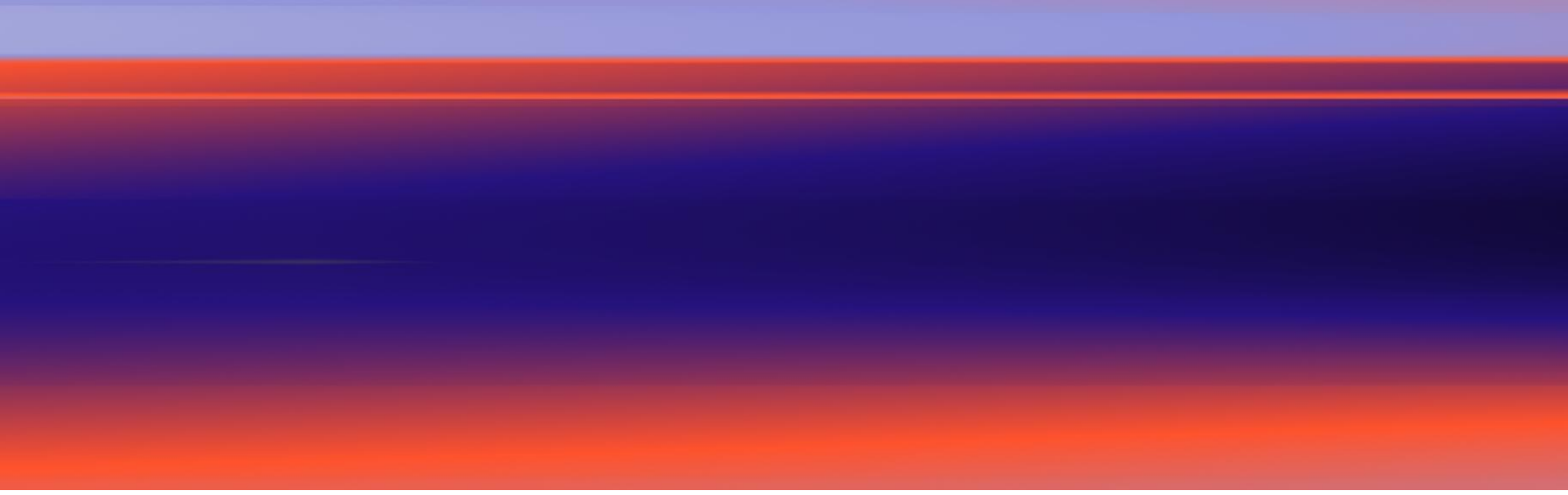
”

"En av de viktigaste lärdomarna är hur avgörande tillit och tydliga beslutsvägar är i en incident."

Rasmus Aveskogh

En av sex Tele2-experter som deltog i Locked Shields 2026, världens största cybersäkerhetsövning med 42 deltagande nationer.

TELE2



4. Hur snabbt kommer ni igång med verksamheten igen?

Förr eller senare inträffar något som kräver återställning, oavsett om det är ett angrepp, ett driftavbrott eller ett enkelt misstag. Skillnaden mellan en dålig dag och en dyr kris ligger i hur snabbt ni är tillbaka i drift igen.

Sommaren 2021 utnyttjade angripare en lucka hos mjukvaruföretaget Kaseya och krävde 70 miljoner dollar i lösensumma. I Sverige fick Coop stänga sina butiker. Coop var inte måltavlan utan drabbades via en underleverantör. Det är alltså fullt möjligt att slås ut av något ni inte rår över, och då avgörs allt av hur snabbt ni kan återställa.

Bra backuprutiner är en billig försäkring, men gå gärna ett steg längre och testa återställningen, inte bara backupen. Skillnaden mellan "vi har backup" och "vi har återställt från backup" upptäcks ofta vid sämsta möjliga tillfälle.

Vad en användbar plan behöver svara på:

- Vilka system måste komma upp först?
- Hur lång tid tar en återställning i praktiken?
- Vem gör vad, och vem fattar besluten?

För det som inte får ligga nere alls finns tekniska lösningar såsom backup som tjänst, och georedundans där data dupliceras på geografiskt skilda platser. Var driften ligger spelar roll här, både för hur snabbt den kan återställas och för vem som har insyn i den.

> "Som svenskt bolag med svensk personal och datacenter i Sverige har vi optimal kontroll över vår infrastruktur, processer och personal."
>
> **Anders Lockner**
> Säkerhetsexpert på Tele2 Företag

Lösningar från Tele2

Backup och återställning, georedundant lagring och säker it-drift med datacenter och support i Sverige, övervakade dygnet runt.

TELE2

Genom hela kedjan: era medarbetare

Som vi redan nämnt är vanor och medvetenhet viktigare än produkter. Men det går inte att agera på något man inte känner till. Därför är utbildning ett av de mest lönsamma skydden som finns. Kunskapen behöver också uppdateras i takt med att hoten ändrar sig. En kort påminnelse gör ofta mer nytta än en grundlig genomgång sällan.

Det är också viktigt att göra det så enkelt som möjligt att agera säkert. Säkerhet som är besvärlig ger upphov till genvägar som privata mejlkonton, eller appar som företaget inte har kontroll över.

Förutom enkelt bör det även vara riskfritt att säga "jag tror jag klickade på något". Den som inte är bekväm med att rapportera kanske väntar, och väntetid kan vara precis vad en angripare behöver.

Ett konkret exempel: säkrare utskick

Vanliga sms utnyttjas dessvärre ofta av bedragare, eftersom avsändaren enkelt kan förfalskas. RCS – nästa generations meddelanden – har verifierad avsändare med namn och logotyp, så era mottagare kan vara säkra på att utskicket faktiskt kommer från er.

Säkerhet handlar inte bara om att skydda er själva, utan också om att era mottagare ska kunna lita på det ni skickar. Läs om hur din organisation kan ha nytta av RCS här.

Var ska ni börja?

Rätt säkerhetsnivå beror på företagets storlek och hur ni arbetar. De flesta börjar med ett starkt grundskydd och lägger till struktur i takt med att verksamheten växer.

	10-99 anställda	99+ anställda
Fokus	Starkt grundskydd, enkelt och kostnadseffektivt	Struktur, styrning och kontroll
Prioritera först	Det som redan ingår, rätt påslaget: flerfaktorautentisering, mejlskydd, testad backup och utbildad personal	Säkerhetsprocesser, incidenthantering och regelefterlevnad
Nästa steg	Trygg molnanvändning och skydd av enheter	Kontinuerlig övervakning och löpande expertrådgivning

Poängen är inte att göra allt på en gång, utan att göra rätt saker i rätt ordning. Se också till att grundskyddet är på plats innan ni bygger mer avancerade lösningar.

Fem frågor hjälper er se var ni står:

- Vilken information skulle skada verksamheten mest om den läckte eller låstes?
- Vilka system måste fungera för att ni ska kunna leverera till kund?
- Vilka krav ställer kunder, partners och regelverk på er?
- Hur snabbt måste ni vara igång igen efter ett avbrott – och klarar ni det idag?
- Vilken kompetens och tid har ni internt, och vad är bättre att lägga ut till en extern leverantör?

Några ord från säkerhetschefen

Säkerhet är en resa, inte en destination. Det är Tele2 Företags säkerhetschef Martin Adetuns motto. Han har genom åren sett att alla typer av verksamheter kan drabbas av cyberattacker – stora som små, nystartade som väletablerade.

Martin Adetuns främsta råd är att lägga tid på riskanalys: tänk igenom vilka hot som skulle kunna inträffa, och hur skyddar ni er mot dem? Se till att säkerhetsfrågor prioriteras och att er verksamhet sätter en tydlig strategi för ert säkerhetsarbete redan från början. Det är bättre att göra vad ni kan, hellre än att ångra att ni inte gjorde mer.

Här kan du ta del av Martin Adetuns checklista kring säkerhet.

TELE2

Tre saker att ha koll på

- **Ai vässar både angrepp och försvar.** Angripare skriver mer trovärdiga nätfiskemejl och hittar luckor snabbare än förr. Samtidigt läser ai-baserat mejlskydd och moderna brandväggar av mönster och stoppar hot innan de når fram. Kapprustningen mellan angripare och försvar gör det starka grundskyddet viktigare än någonsin.

- **Regelkrav har blivit lag.** Den 15 januari 2026 trädde cybersäkerhetslagen i kraft och förde in EU:s NIS2-direktiv i svensk rätt. Den omfattar 18 sektorer och kräver bland annat systematiskt säkerhetsarbete och incidentrapportering. Men kraven sprider sig vidare: de som omfattas av lagen måste även kunna svara för sina underleverantörer. Lagen kan alltså nå er via en kund.

- **Trygghet blir ett säljargument.** Nästan hälften av beslutsfattare och chefer inom it anser att svenska företag investerar för lite i säkerhet. Att vara ett av de företag som faktiskt satsar på säkerhetsarbetet kan därmed bli till en konkurrensfördel. Kunder vill veta att deras uppgifter hanteras säkert, och ett strukturerat säkerhetsarbete med data som stannar i Sverige väger allt tyngre i upphandlingar.

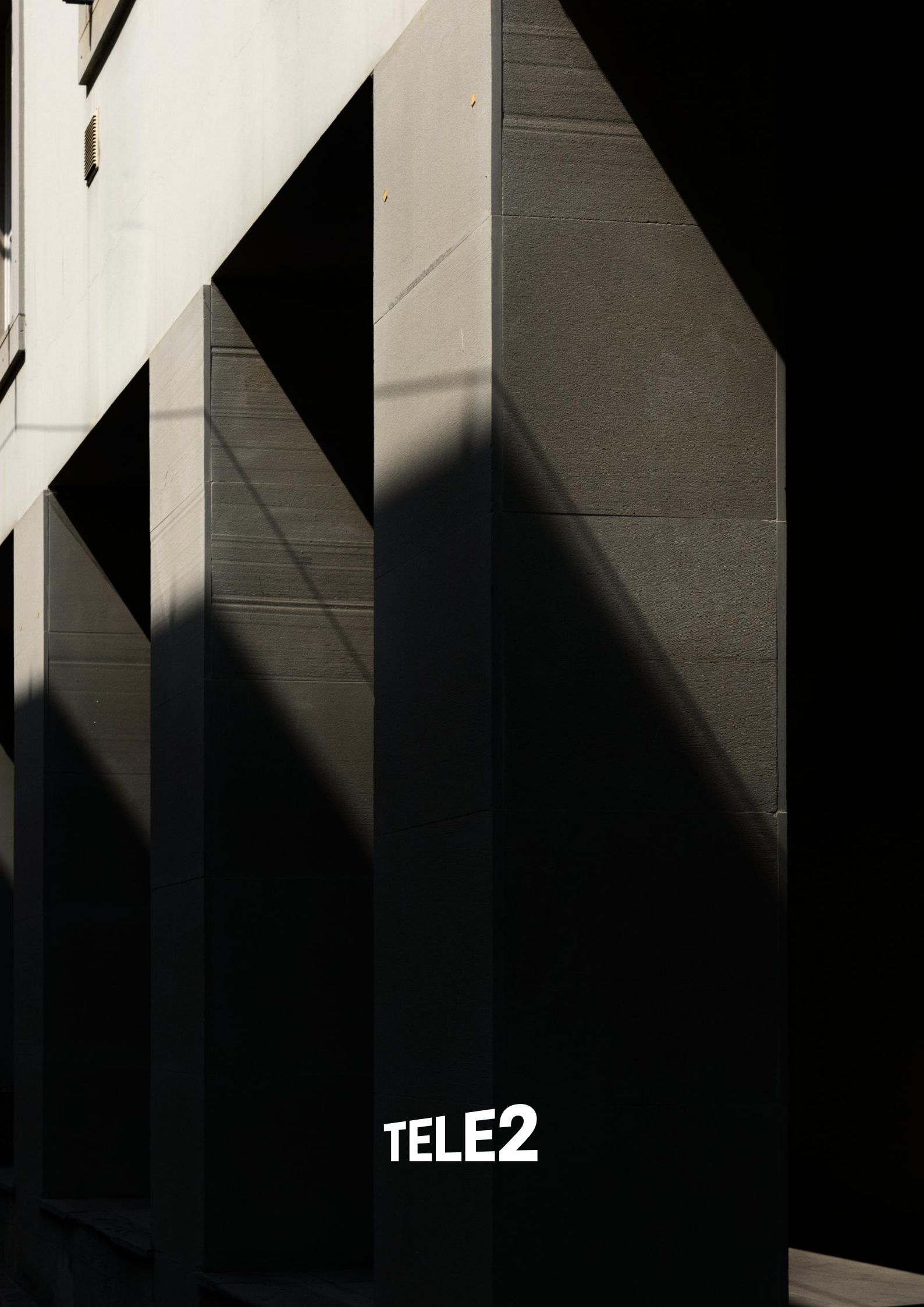
Nästa steg

Ett bra säkerhetsarbete börjar inte med att köpa teknik. Det börjar med att förstå nuläget och prioritera rätt.

Tele2 kan hjälpa er hela vägen, från kartläggning av behoven till val och drift av rätt lösningar. Både datacenter och support finns i Sverige, och den hårdvara vi ansvarar för tas om hand cirkulärt med klimatberäkning enligt Greenhouse Gas Protocol.

Vill ni veta var ert företag står idag? Boka en kostnadsfri rådgivning på tele2.se/foretag/radgivning så hjälper vi er vidare.

TELE2


TELE2