Telia | Telia Cygate

Är du säker?

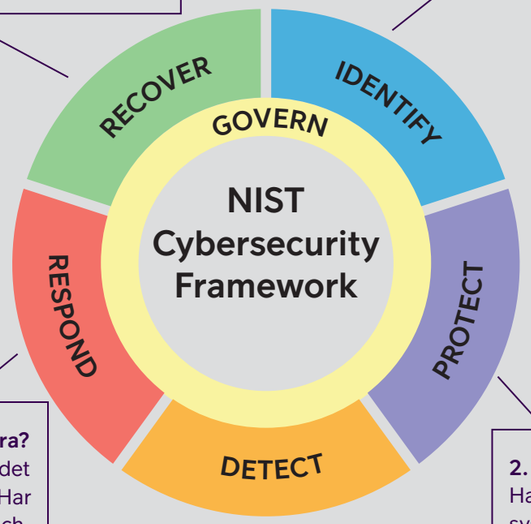
Förstå hoten, minimera riskerna och var redo för det oväntade

Det här är NIST CSF

Vi på Telia Cygate hjälper våra kunder att arbeta strukturerat med säkerhet genom NIST CSF. Ramverket gör det lättare att prioritera säkerhetsfrågor, identifiera sårbarheter och bygga ett effektivt skydd. Det säkerställer också att angrepp snabbt upptäcks, att rätt åtgärder sätts in och att lärdomar tas tillvara för att stärka skyddet framåt. Förutom att bygga ett tekniskt försvar, behövs även löpande styrning av vad som ska skyddas, varför det är viktigt, och vem som är ansvarig. Ramverket bidrar till bra beslut och långsiktig trygghet.

1. Är du säker på vad du skyddar?
Innan du kan säkra något, måste du förstå vad som behöver skyddas och vilka risker som finns. Har ni identifierat affärskritiska tillgångar, känslig data och sårbara system?

5. Är du säker på att du kan återställa?
När incidenten är över måste verksamheten snabbt komma tillbaka. Kan ni lita på er backup och återställningsplan?



4. Är du säker på att du kan agera?
När attacken är ett faktum gäller det att reagera snabbt och effektivt. Har ni en plan för incidenthantering och tydliga ansvarsområden?

2. Är åtkomsten säker?
Har rätt personer rätt tillgång till system och infrastruktur – och ingen annan? Säker autentisering och smarta accesskontroller skyddar både användarna och organisationen.

3. Är du säker på att du ser hot och avvikelser?
Attacker sker i det dolda. En bra övervakning gör att du kan upptäcka och stoppa hot och avvikelser innan skadan är skedd.

Dags att rusta för robusta säkerhetskedjor

Vi lever i en tid där säkerhet inte längre är en teknisk fråga, utan en strategisk nödvändighet. Cyberhot och geopolitisk instabilitet påverkar oss alla, från individnivå till nationell säkerhet. Totalförsvar handlar inte bara om militära resurser, utan om att företag, myndigheter och enskilda individer tar ansvar för att bygga en motståndskraftig och säker digital infrastruktur.

Människan är och förblir den största attackvektorn. Vi klickar snabbare än vi tänker, använder för svaga lösenord och faller för alltmer sofistikerade AI-genererade bedrägerier. Vi kan aldrig göra oss immuna mot den mänskliga faktorn, men vi kan bygga system som kompenserar för den.

Lösningen ligger inte i fler isolerade säkerhetsprodukter, utan i integrerade plattformar och arkitekturer som minskar komplexitet och täpper igen säkerhetshål. System som snabbt kan agera på hotintelligens och som fungerar även under kris. Det handlar om att bygga robusta säkerhetskedjor som håller, även när en kabel kapas i Östersjön.

På Telia Cygate har vi en unik position. Som en del av Telia ser vi hotbilden i den svenska IT-infrastrukturen på ett sätt som få andra gör. Vi kan skapa slutna system där kritisk data skyddas hela vägen, från en enskild enhet till applikationer i säkra molnmiljöer.

När någon frågar om du är säker, hoppas jag att du svarar: Jag arbetar för att vara det. Det betyder att du gör ditt bästa för att bygga en förståelse för hoten och minimera riskerna, och att du bygger en organisation som är redo att hantera det oväntade.

Fredrik Sidmar
VD, Telia Cygate

IDENTIFIERA
Kartlägg organisationens tillgångar, risker och sårbarheter för att skapa en grund för ett effektivt säkerhetsarbete.

Är du säker på vad du skyddar och vilka hot som finns?

Hur stark är den svagaste länken i er säkerhetskedja?

Det nya NIS2-direktivet speglar den förvärrade hotbilden och manar fler företag och organisationer att ta större steg mot att öka robusthet och motståndskraft. NIS2 förstärker vikten av att ledningen är aktiv i sitt arbete med försvarsviljan hos den egna organisationen, för att utbilda sig själva och sina medarbetare.

”Även om man inte tycker att man träffas av NIS2 så bör man fråga sig: Har vi råd att bli av med all vår data? För med ransomware-attacker är det allt eller inget”, säger Adam Önder, säkerhetsarkitekt på Telia Cygate.

Ofta är en bra plats att börja att informationsklassa, eller inventera sin data och sina övriga tillgångar som ett första steg, och utse någon eller en grupp personer med tentakler i verksamheten som får i uppgift att driva frågorna framåt.

”Den största risken av alla, är att inte ens veta om sina risker. Skyddet är aldrig starkare än den svagaste länken.”
Adam Önder, Säkerhetsarkitekt, Telia Cygate.

”Om cyberbrottslighet hade varit en bransch som ägnade sig åt lagliga saker hade vi imponerats av deras innovationskraft, nytänkande och tempot i utvecklingen. Nu ser vi den växande industrin som ett hot mot ett fungerande samhälle.”

Michael Mothander, Strategisk portföljägare, säkerhet, Telia Cygate.

”Den som har varit med om en större attack glömmer det aldrig. Jag kan känna pulsen öka när jag tänker på händelser jag varit med om.”

Per Josefsson, Systematiskt säkerhetsarbete, Telia.

Spana som en cyberbrottsling

Ett penetrationstest är en manuell simulering av ett dataintrång. Företag och organisationer anlitar ett team IT-säkerhetsspecialister, vanligast benämnt Pentest-team, med många års erfarenhet för att hacka deras system för att identifiera svagheter innan cyberbrottslingar nyttjar dem.

”Alla lär sig mycket under ett penetrationstest. Man får svart på vitt vad som är bra idag och vilka områden som man behöver stärka upp”

Christian Holmstedt, Specialist cybersäkerhet och IT-säkerhet, Telia Cygate

Så skapas sårbarheter

IT-system är stora och komplexa och drabbas över tid av något som kallas ”konfigurationsförfall”. Det kan räcka med en liten konfigurationsmiss för att dörren ska ställas på vid gavel. Och i värsta fall är håller cyberbrottslingarna koll och väntar på att det ska hända.

Zero trust

Zero Trust är en säkerhetsmodell där ingen användare eller enhet automatiskt får förtroende, oavsett om de befinner sig inom eller utanför nätverket. Genom verifiering, segmentering och minimering av behörigheter minskar risken för intrång och dataläckor.

Andelen som uppger att de kan identifiera vilka risker som finns för att interna system ska utsättas för intrång*:

Lågdigitala:
16%

Mellandigitala:
33%

Högdigitala:
46%

* Siffrorna kommer från Telias Digitala Index 2024 som bygger på en undersökning som genomförts av analysföretaget Nepa. Frågor har ställts till beslutsfattare eller personer som har avgörande inflytande över valet av leverantör inom IT, telekom och digitala tjänster på cirka 1000 svenska företag. Undersökningen genomfördes i januari – februari 2024

SKYDDA
Implementera säkerhetsåtgärder för att förhindra incidenter och minimera skador genom exempelvis accesskontroll, kryptering och medvetenhetsträning.

Är åtkomsten säker?

Två kilobyte som kan sänka webben

I många situationer behöver vi kunna styrka att vi är den vi utger oss för att vara. I den fysiska verkligheten använder vi till exempel körkort, och på nätet är certifikat ett exempel på en digital identitet.

”Det är svårt att greppa att någonting som är så litet som 2kb kan få så stora konsekvenser. Och om det är lite rörigt bland era certifikat är ni långt ifrån ensamma om det.”

Sandra Larsson, Tjänsteägare, Telia Cygate.

Ett utgånget certifikat kan leda till att det plötsligt inte går att handla på en e-handelssajt eller att medborgare inte kan ta del av kommunens e-tjänster. Men trots att trassel med certifikat är relativt vanligt, och leder till många kostsamma och störande avbrott, råder det hos många verksamheter osäkerhet kring statusen på beståndet av certifikat.

”Det är svårt att greppa att någonting som är så litet som 2kb kan få så stora konsekvenser. Och om det är lite rörigt bland era certifikat är ni lång ifrån ensamma om det”, säger Sandra Larsson, Tjänsteägare, Telia Cygate.

Släppa ut industrinät på internet?

Inom industrin är det ingenting nytt att koppla samman maskiner i produktionsnät (OT-nät) så de kan samarbeta med varandra. Nu ökar trycket att koppla upp OT-näten mot internet eftersom data som genereras i verksamheten blir en värdefull tillgång. Möjligheterna som kommer med uppkoppling är oändliga, men samtidigt öppnas dörren till en mängd faror på utsidan.

”Här har vi en marknad med stor potential, men företag behöver ta sig an digitaliseringen på ett klokt sätt och förstå risken man utsätter sig för om man kopplar upp maskiner med gamla operativsystem, säger Jonathan Grimmtjärn, IT- och nätverksarkitekt, Telia Cygate.

”Vilka säkerhetsåtgärder ett företag bör införa beror på vilken hotbild mot verksamheten som föreligger i förhållande till vad de anser skyddsvärt eller känsligt.”

Tomas Eklind, Taktisk portföljägare, säkerhet, Telia Cygate.

DDoS - Attack eller avledning?

Visste du att en överbelastningsattack, Distributed Denail-of-Service (DDoS), kan syfta till att skapa allmän oreda inför att en hotaktör i nästa steg avser att angripa verksamheten på ett annat sätt? DDoS-attacker syftar i andra fall till att störa eller att lära känna svagheter hos den utsattes verksamhet.

Hjälpsamhet är ett säkerhetshot

Våra kollegor och medarbetare har en stark drivkraft att möta förväntningar från kunder, kollegor och chefer. Ibland kan en hjälpsam person bryta mot organisationens säkerhetspolicy för att få jobbet gjort. Som att dela dokument via osäkra plattformar eller ansluter till ett osäkert nätverk för att delta i ett möte.

”Det måste vara lätt att göra rätt och alla behöver ha koll på sin attackyta. Man kan ha världens säkraste policy, men om organisationen inte följer den så spelar det ingen roll”, säger Claes Olsson som arbetar som IT-säkerhetsarkitekt på Telia Cygate.

”Det måste vara lätt att göra rätt och alla behöver ha koll på sin attackyta. Man kan ha världens säkraste policy, men om organisationen inte följer den så spelar det ingen roll”

Claes Olsson, IT-säkerhetsarkitekt, Telia Cygate.

Andelen som svarar att de kan skydda och säkerställa att kritiska verksamhetsfunktioner kan levereras*:

Lågdigitala:
20%

Mellandigitala:
45%

Högdigitala:
57%

* Siffror från Telias Digitala Index 2024.

STYRA
Governance, eller styrning, handlar om att skapa riktning, ansvar och sammanhang.

Är du säker på att ni styr rätt?

Strategi utan styrning blir lätt en pappersprodukt. Governance handlar om att skapa struktur, ansvar och riktning, så att säkerhetsarbetet faktiskt händer. Är säkerheten en integrerad del av beslutsfattandet hos er? ”Många tror att de har governance bara för att det finns en strategi. Men om teknikerna inte vet varför de gör något, eller cheferna inte följer upp, så saknas styrning”, säger Claes Olsson, Säkerhetsarkitekt Telia Cygate.

Trafikregler för säkerhetsarbetet

En bra bild är att se governance som ett trafiksystem. När farten ökar, fordonen blir fler och vägarna mer komplexa räcker det inte längre med bara stoppskyltar. Vi behöver rödljus, rondeller och upplysta vägskyltar, och alla bilister behöver känna till och följa reglerna.
”Visst, det är enklare att köra hur man vill. Men då ökar också risken att det smäller. Governance är bromsarna, skyltarna och vägmarkeringarna som gör att vi kan köra säkert samtidigt som vi håller hög fart”, säger Adam Önder, Säkerhetsarkitekt Telia Cygate.

Andelen som anser att de har tydliga roller, ansvar som policies och rutiner för systematiskt säkerhetsarbete*:

Lågdigitala:
25%

Mellandigitala:
46%

Högdigitala:
63%

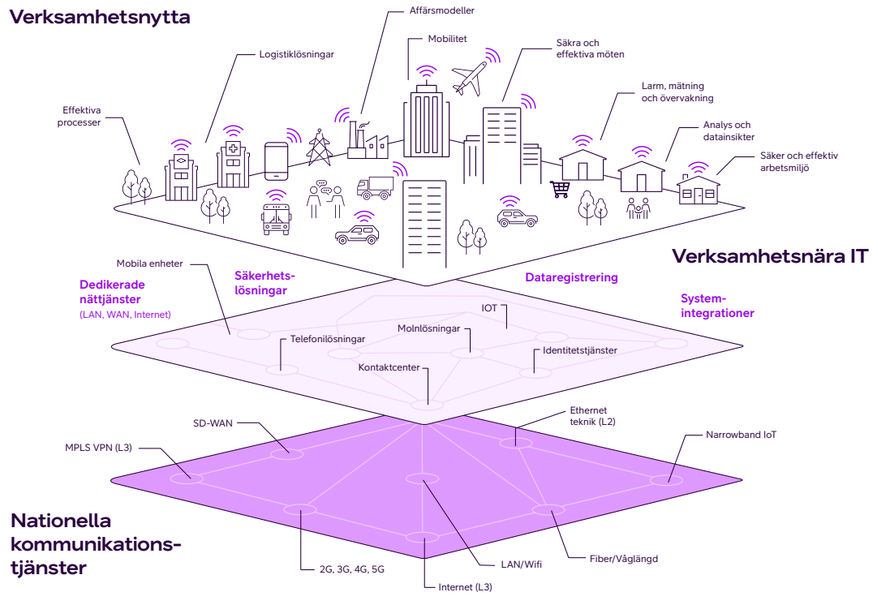
* Siffror från Telias Digitala Index 2024.

Säker digitalisering
Få det att fungera, eller fokusera på att innovera?

Många företag brottas med utmaningen att möta kundernas krav samtidigt som de måste hantera en alltmer komplex digital verklighet. För vissa innebär det att optimera produktionen för att maximera utvinningen av råvaror, för andra handlar det om att skapa en smidigare och mer engagerande kundupplevelse. Oavsett bransch krävs en stabil, sammanhållen och säker teknisk grund för att kunna anpassa sig och fortsätta vara konkurrenskraftig.
En robust och suverän infrastruktur är nyckeln till att hantera utmaningarna. När tekniken fungerar som den ska blir den en katalysator för innovation och tillväxt. Ett gruvbolag som vill öka malmproduktionen behöver ett system där maskiner och självkörande fordon kan arbeta sömlöst tillsammans. Ett logistikföretag måste säkerställa att varuflöden optimeras med realtidsdata, utan att informationen exponeras för osäkra nätverk. En e-handelsplattform som vill stärka sin kundlojalitet behöver en digital upplevelse utan störningar, där transaktionsdata skyddas i varje steg av processen.

Robust, säker och suverän

Med en suverän infrastruktur där säker datahantering, säker konnektivitet och verksamhetskontinuitet samverkar, skapas den trygghet och stabilitet som krävs för att driva verksamheten framåt.
Företag som fokuserar på att själva hantera den underliggande tekniken riskerar att tappa fart när marknaden förändras. Att i stället fokusera på att tillämpa tekniken på ett strategiskt sätt gör det möjligt att bli snabbare, mer anpassningsbar och att utveckla nya tjänster som stärker konkurrenskraften. Genom en suverän infrastruktur med end-to-end-säkerhet kan företag skicka och hantera data på ett sätt som är både säkert och effektivt, utan att vara beroende av internet.
Den avgörande frågan för alla företag och organisationer är om man vill vara en aktör som arbetar med teknik, eller en som nyttjar teknik för att driva affären framåt.



Med en flexibel, säker och verksamhetsunik bottenplatta för IT-infrastruktur och datakommunikation kan företag minimera riskerna och upprätthålla både säkerhet och prestanda, samtidigt som fokus ligger på digitaliseringsinitiativ som skapar verksamhetsnytta och konkurrenskraft.

UPPTÄCKA
Övervaka och identifiera säkerhetshot i realtid för att snabbt kunna agera vid misstänkta aktiviteter.

Är du säker på att du ser hoten?

Säkerhetsexperter gör realtidsanalys

Ett Security Operations Center (SOC) är en centraliserad enhet som övervakar och hanterar den egna organisationens eller kunders it-infrastruktur från ett cybersäkerhetsperspektiv. Arbetet syftar till att proaktivt skydda system, känna igen attacker, som hela tiden blir alltmer sofistikerade, och minimera skador vid cyberattacker.

Säkerhetsexperter som arbetar i en SOC:en använder en rad olika verktyg för att övervaka, analysera och reagera på säkerhetsincidenter. De samlar in och analyserar loggar från olika system och applikationer för att hitta avvikande mönster som kan tyda på incident.
”Vi skyddar våra kunders IT-miljöer mot en rad olika typer av cyberhot, som exempelvis malware, ransomware och phishing-attacker”, säger Martin Spiik, Head of Security Services, Telia Cygate.

Mångfald av perspektiv ger bäst skydd

En SOC är organiserad för att säkerställa en holistisk och effektiv hantering av cyberhot. I ett team behöver man ha en blandning av erfarenheter och färdigheter för att kunna ta hand om olika aspekter av cybersäkerhet. Som exempelvis teknisk kompetens, branschkännedom, förståelse för hotlandskapet och förmågan att snabbt anpassa sig till nya hot och teknologier.

”En bredd av bakgrunder och perspektiv stärker vår förmåga att möta och lösa komplexa cybersäkerhetsutmaningar.”

Martin Spiik, Head of Security Services, Telia Cygate

Den som inte vet är inte säker

För att identifiera hot i ett tidigt skede behöver det finnas verktyg och processer för kontinuerlig övervakning, hotdetektering och sårbarhetsskanning. Genom att analysera nätverkstrafik och systemloggar kan misstänkta aktiviteter upptäckas snabbt. Målet är att minska tiden från intrång till åtgärd och begränsa skador vid en attack.

”Vi tränar på de olika scenarierna så att vi kan hålla huvudet kallt och hjälpa våra kunder när det är en attack. Då gäller det att ha is i magen och fatta beslut utifrån fakta.”

Huda Khan, Strategi och kvalitet av leverans, Telia Cygate.

”Utredningsarbete kräver mycket resurser och det är viktigt att snabbt kunna avskriva händelser som på ytan ser ut som hot och kunna förklara varför en regel har löst ut.”

Fredrik Johansson, Upptäcka hot och stärka försvar, Telia Cygate.

Analysera från angriparens perspektiv

För att skydda oss på rätt sätt behöver vi förstå vad som är skyddsvärt, som känslig information eller kritiska system, eller verksamhetens leveransförmågor. Vi behöver skaffa oss en bild över vilka våra potentiella angripare är och hur de vanligtvis agerar, samt kartlägga vår verksamhets externa fotavtryck. För de spår vi lämnar efter oss kan utgöra lågt hängande frukter för en angripare, och genom att bättre förstå hur vi ser ut i deras ögon kan vi skydda oss på ett bättre sätt.

Andelen som säger att de kan upptäcka intrångsförsök och hot*:

Lågdigitala:
28%

Mellandigitala:
48%

Högdigitala:
56%

* Siffror från Telias Digitala Index 2024.

REAGERA
Utveckla och genomför en handlingsplan för att effektivt hantera och begränsa skador vid en säkerhetsincident.

Är du säker på att du kan agera?

När cyberattacken är ett faktum

Om du pratar med någon som har varit med om en allvarlig cyberincident så kommer de flesta berätta om en överväldigande känsla av stress och chock. Att utsättas för en attack upplevs av många som att få ett plötsligt slag i ansiktet, och det vet hotaktörerna om. Därför trycker de ofta ut sina krav tidigt under hanteringsprocessen när de vet att de som drabbats fortfarande är paralyserade av stress.

”Hotaktörer ägnar sig både åt teknisk och psykologisk krigföring, och vi arbetar med försvaret på samma sätt”, säger Joakim Lidén Incidenthantering, Telia Cygate.

Akutteam som arbetar med teknik och samordning

För att ta ett helhetsgrepp om arbetet med hantering av incidenter består Telia Cygates incident response team av medarbetare med två kompletterande roller: incident responders och incident response managers. Tillsammans har de kompetens och förmåga att hantera både teknik och människor på bästa sätt. När de kallas in drar ett väloljat maskineri igång. Incident responders börjar samla in digitala fotspår medan incident response managers sätter igång att skapa en överblick och samordna insatser.

> **”När man inte vågar prata öppet om det som inträffat riskerar man att agera förhastat och fatta panikbeslut, men man går också lätt miste om lärdomar som kan vara värdefulla för att stärka säkerheten framåt.”**
>
> Joakim Lidén, Incidenthantering, Telia Cygate

”Vi jobbar som ett akutteam. Först stoppar vi blödningen och sedan arbetar vi på den långsiktiga lösningen. Våra incident responders är otroligt uppskattade under kriser eftersom de är tekniskt skickliga och bra på att kommunicera”, berättar Joakim Lidén.
Målet är att få tillbaka kundens digitala miljö till ett normalläge så snabbt det bara går. För att nå dit måste det först etableras ett gott samarbete mellan alla parter så att det går att arbeta metodiskt. Att hitta kryphål är ofta lättare att än att täppa till dem. Joakim beskriver det som en katt och råtta-lek som hela tiden blir mer avancerad.

”För mig känns det meningsfullt att vara den som hjälper till och skapar lugn i en utmanande situation”, säger Joakim Lidén.

Från kris till stärkt säkerhet

Det är vanligt att de som drabbas av cyberbrott känner ett visst mått av skam. Det kan både drabba individer, exempelvis den som klickat på en osäker länk och öppnat för angreppet, men också organisationer som helhet.

”När man inte vågar prata öppet om det som inträffat riskerar man att agera förhastat och fatta panikbeslut, men man går också lätt miste om lärdomar som kan vara värdefulla för att stärka säkerheten framåt”, säger Joakim Lidén.

För Joakim och hans kollegor är det självklart att aldrig leta syndabockar under hanteringen av en incident, utan att arbeta strukturerat för att lösa det aktuella problemet och minimera skadan.

”Självklart vill vi hitta rotorsaken till en säkerhetsincident, och med rätt hjälp tar man sig genom cyberattacken och kommer ut starkare på andra sidan”, säger Joakim.

När det hettar till i SOC:en

Ett Security Operations Center (SOC) är en övervakningsstyrka som kontinuerligt tittar på säkerhetshändelser. När larmet går är de redo att agera, och självklart hettar det till på SOC:en vid ett larm, men för det mesta finns det en naturlig förklaring.

Som att kunden glömt att berätta att de skaffat en programvara för att scanna och kartlägga alla enheter på nätverket, eller att någon spillt kaffe på tangentbordet och råkat flytta ett stort antal filer från en mapp till en annan när de torkade upp.

Andelen verksamheter som svarar att de kan hantera och agera på intrång och upptäcka hot*:

Lågdigitala:
24%

Mellandigitala:
34%

Högdigitala:
44%

* Siffror från Telias Digitala Index 2024.

ÅTERSTÄLLA
Säkerställ snabb återhämtning efter en attack genom att återställa system, förbättra säkerhetsrutiner och minska framtida risker.

Är återställningen säker?

En katastrof kan se ut på många olika sätt. Exempelvis en brand i ett datacenter eller en ransomeware-attack som förlamar hela verksamheten. När krisen är ett faktum handlar allt om att så snabbt som möjligt återställa en fungerande infrastruktur och verksamhet.

5 tips på förebyggande åtgärder

1. Backup och återläsning
Säkerställ att dina rutiner för backup och återläsning fungerar, testa regelbundet.
För data och information som är verksamhetskritisk, etablera säkra backuplösningar

2. Säkerhetsteam i beredskap
Ett förberett säkerhetsteam (IRT, Incident Respons Team) som vet hur de ska agera under stress och press kan göra stor skillnad för hela verksamheten. Om möjligt, säkerställ tillgången av ett IRT och träna på fiktiva cybersäkerhetsincidenter inom organisationen.

3. Kommunikationsplan
Vänta inte med att skriva planen, börja nu! Har du redan en plan som är bra på pappret, testa den genom en intern övning där intressenter får agera i ett fiktivt scenario. Det kommer löna sig och förmodligen kommer ni hitta förbättringspotential under själva övningen.

4. Lärdomar
Skapa en rutin för att analysera inträffade cybersäkerhetsincidenter. Vid behov dra nytta av IRT för att genomföra workshops där IT och verksamhet proaktivt identifierar och dokumenterar gemensamma lärdomar. Tillsammans kommer ni skapa en mycket bättre framtida motståndskraft.

5. Återuppbygg förtroende
Underskatta inte betydelsen i att återuppbygga förtroendet. Det kan också handla om att stötta enskilda individer som haft stort tryck på sig under återställningsarbetet. Bekräfta lärdomarna och investera tid där det behövs, både internt och externt.

”När katastrofen är ett faktum vill man att allt man planerat ska fungera som ett väloljat maskineri. ”

Zakaria Bennani, Strategisk portföljägare, hybrida moln, Telia Cygate.

Andelen som uppger att de kan återställa kritiska verksamhetsfunktioner efter angrepp*:

Lågdigitala: **16%**

Mellandigitala: **26%**

Högdigitala: **33%**

* Siffror från Telias Digitala Index 2024.

Är du säker?

Säkerhet är inte något statiskt utan en ständig rörelse. Cyberbrottslingar utvecklar sina metoder, och förr eller senare kommer din organisation att utsättas. Ska man bara ge upp? Finns det en enkel lösning?

Nej.

Säkerhet kräver att du ligger steget före, hittar rätt balans mellan skydd och verksamhetsutveckling, och är redo när hotet blir verklighet.

I den här broschyren visar vi hur man kan stärka säkerheten med hjälp av ramverket NIST. Du får insikter från experter, en förståelse för hotbilden, och konkreta råd om hur du bygger motståndskraft. Det handlar inte om att vara perfekt, utan om att hela tiden röra sig framåt.

Teliacygate.se

Telia | Telia Cygate