20221129015548

TRIPNET

Årsredovisning

för

Tripnet AB

556507-5362

Räkenskapsåret

2021–05–01 – 2022–04–30

Fastställelseintyg

Undertecknad styrelseledamot i Tripnet AB intygar att resultaträkningen och balansräkningen i årsredovisningen har fastställts på årsstämma 2022-10-31. Årsstämman beslutade att godkänna styrelsens förslag till resultatdisposition.

Jag intygar också att innehållet i årsredovisningen, revisionsberättelsen och övriga bifogade handlingar stämmer överens med originalen.

Göteborg 2022-10-31

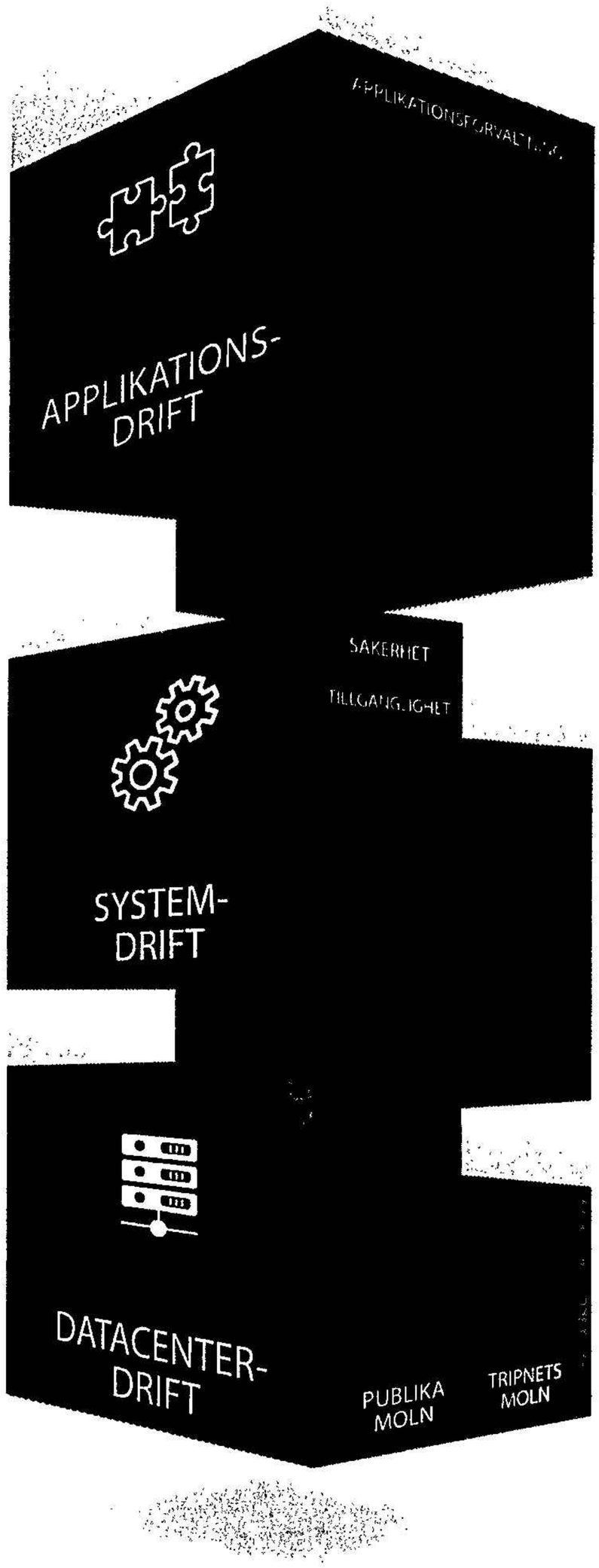
Ulf Persson

549

ÅRSREDOVISNING 2021 / 2022

20221129081350

Vi är Tripnet



Tripnet levererar modern IT-drift för kunder som prioriterar hög säkerhet och tillgänglighet. Vi finns för dig som värdesätter personliga relationer, vill bli sedda, söker insiktsfulla råd och uppskattar vårt ansvarstagande.

Tripnet har kontor och datacenter i Göteborg. Sedan starten 1995 har vi utvecklats till experter på såväl informations- och cybersäkerhet som avancerade driftslösningar.

Våra kunder är såväl multinationella industriföretag som handelsföretag, myndigheter och organisationer, som uppskattar personliga kontakter och långa relationer.

20221129015511

Nyckeltal

> Vi vet hur man säkerställer rätt säkerhetsnivå för affärs- och samhällskritiska IT-system i såväl, publika molntjänster som Tripnet Cloud och datacenter.

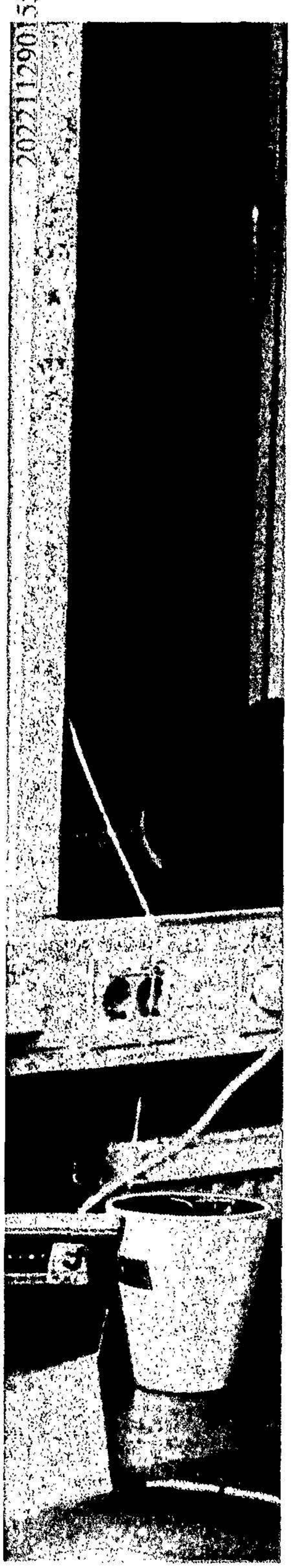
Flerårsöversikt (tkr)	2021/22	2020/21	2019/20	2018/19	2017/18
Nettoomsättning	57 915	64 968	59 003	59 203	52 634
Resultat efter finansiella poster	617	6 122	2 185	2 503	2 312
Balansomslutning	28 362	27 710	22 413	23 189	27 105
Soliditet (%)	27	36	30	29	22

För definitioner av nyckeltal, se Redovisnings- och värderingsprinciper.

Vi är ett relations- och kunskapsintensivt företag med fokus på säkerhet och systemdrift. Tripnet är specialister som kombinerar nyfikenhet och djup kunskap inom informations- och cybersäkerhet med att också vara versatilister med en bred och djup kompetens kring hur man skapar och upprätthåller säker drift dygnet runt.

Vår målgrupp är medvetna kunder med höga krav på bevisad *tillgänglighet, konfidentialitet och integritet, samt kunder* med krav på säkerhetsskydds-klassade system. Vi vet hur man säkerställer rätt säkerhetsnivå för affärs- och samhällskritiska IT-system i såväl, publika molntjänster som Tripnet Cloud och datacenter.

Ulla Persson



VD har ordet

När pandemin äntligen såg ut att vara under kontroll, när restriktionerna var släppta och vi kunde återgå till jobbet – då invaderades Ukraina av Ryssland. Jag trodde att världen hade lärt sig något av pandemin?

Att vi skulle kunna gå vidare, fokusera på klimatkrisen och tillsammans försöka lösa våra globala utmaningar. Men, nu kommer jag i stället att tänka på Albert Einstein som sa " – Endast två saker är oändliga: universum och mänsklig dumhet. Och vad gäller universum är jag är inte säker."

Vardagen har återgått till något som känns lite mer normalt. Kollegorna är tillbaka på kontoret. Jag stöter på kunder och partners som är på besök. Fysiska kundmöten är inbokade i kalendern och energifyllda lunchmöten lockar. Samtidigt ligger det med en Teamslänk i de flesta möten. Vi kombinerar distansarbete och arbete på kontoret utifrån kunders, kollegors och våra individuella behov. Jag är övertygad om att det gör att vi alla får ett mer harmoniskt arbetsliv och lättare att få ihop livspusslet. Det känns som om vi alla har lärt oss mycket av pandemin!

Vi är säkra på att säkerhet måste vara i fokus

Säkerhet har alltid varit en viktig del av vår verksamhet, men frågan har i stort bytt karaktär sedan vi startade 1995. Läs gärna Martins retrospektiva reflektion på sidan 16. Vi har de senaste åren ökat vårt verksamhetsfokus på säkerhetsfrågor för att kunna hjälpa våra kunder med allt från informationssäkerhet, via cybersäkerhet, till klassisk IT-säkerhet. Vi har lanserat några nya tjänster, bland annat för detektering av illvilliga operationer. Idag räcker det inte alltid med förebyggande skydd. Du behöver även hantera situationen om – eller kanske när – ett dataintrång lyckas. På sidan 10 kan du läsa mer om när det hände oss ... För att i möjligaste mån undvika oönskade situationer är det viktigt att arbeta strukturerat med säkerhet, där det övergripande är informationssäkerhet.

20221129015534

På sidan 20 berättar vår informationssäkerhetsansvarige Marcelo mer om vad man kan och bör göra.

På Tripnet har vi arbetet med säkerhet och kvalitetssystem sedan 1996. De senaste åren har vi utgått från vårt ledningssystem för informationssäkerhet och ISO 27000. På sidan 26 berättar Göran Sjöberg om hur vi i skrivande stund arbetar med vår certifiering. Om du är nyfiken berättar jag gärna mer om du tittar förbi på en kopp kaffe.

Tripnets erbjudande i ständig utveckling

- EDR

Som en effekt av vårt starka fokus på säkerhet föll det sig helt naturligt att utveckla en ny tjänst för att upptäcka, analysera och åtgärda oönskade aktiviteter (MalOps) på servrar. Att tidigt upptäcka avancerade försök till intrång i en IT-miljö är nyckeln till att göra säkerhetsåtgärder och säkerställa ett fortsatt fullgott skydd. Med vår nya tjänst EDR övervakas system kontinuerligt om det förekommer okända eller oönskade aktiviteter. En systemingenjör på Tripnet gör en bedömning och kan snabbt vidta åtgärder. Lösningen är dessutom modernt kryddad med AI och automation.

- Tripnet Cloud

Vi har dessutom lanserat en ny version av Tripnet Cloud, med möjlighet till större servers, vilket bland annat ger möjligheter till bättre licensutnyttjande. Vi har även lanserat en ny version av vår självprovisioneringstjänst, som ger de kunder som har behov av att själv hantera sina servers en än mer flexibel miljö.

- Databaskluster

För att öka tillgängligheten på traditionella enterprisesystem har vi vidareutvecklat våra tjänster för fysiska databaskluster. Databaskluster byggs för att säkerställa att data är tillgänglig om ett fel inträffar. Det kan vara maskinvaru- eller programvarufel, nätverksanslutningsproblem eller mänskliga misstag. Oavsett störningar i datorhall, server eller lagring, kan vi leverera funktioner som passar kundens organisationsbehov, baserat på skyddsnivån och SLA-krav.

- Säkerhetstjänster

Vi fortsätter förstås att utveckla vår tjänsteportfölj med fokus på informations-, cyber- och IT-säkerhet. Tripnet är och fortsätter vara ett relations- och kunskapsintensivt företag med fokus på säkerhet och systemdrift. Vi levererar insiktsfulla råd kring alla våra kunskapsområden!

Fortsatt förtroende och nya kunder

Vi har under året fått förnyat förtroende från flera av våra större kunder, bland annat ett av Sveriges ledande fastighetsbolag och ett ledande säkerhetsföretag. På nykundssidan kan vi hälsa Skandinaviens ledande företag inom "lyfta högt, bygga rejält och förvalta smart" välkomna. De har dessutom ett starkt grönt fokus som vi gillar. Vi har även fått företaget bakom en av Sveriges mest populära e-handelslösningar som kund. Det känns extra spännande, eftersom vi hade ett utvecklingssamarbete med dem redan i slutet på 90-talet. Hjärtligt välkomna tillbaka! Vårt mångåriga samarbete med en av Sveriges största och äldsta speloperatörer har vidare utvecklats. Samtidigt har vi fått förtroende att hantera de system som ska förhindra spelmissbruk på spelbolag med svensk licens.

Kommer hållbarhet sättas på undantag ända till 2025?

När utvecklingen i stora delar av världen går bakåt, förutspås fokus på hållbarhet hamna i skymundan. Jag har hört det

Ulf Persson

20221129013536

från bland annat Hans Werner på analysföretaget Radar, som är en ständigt återkommande gäst på vår årliga Kunskapsfrukost med framtidstema. Tendensen känns inte alls bra! På Tripnet har vi en grön framtidsvision och ett helhetsperspektiv kring hållbarhet. Vi tar ansvar för såväl ekonomiska som sociala och ekologiska aspekter av hållbarhet. Därtill är vi övertydliga med att Tripnet ska vara en arbetsplats där alla accepteras och får utrymme att utvecklas. Tolerans och öppenhet är en del av vår företagskänsla och vi vet att mångfald är en framgångsfaktor. Då är det inte ok att pausa hållbarhetsarbetet. Låt oss hjälpas åt att skippa den trenden, ok?

Ett ännu vassare ledningsteam och tillspetsad organisation

Vi har under året utvecklat såväl sammansättning som arbetsmetodik i ledningsteamet för att bli effektivare och snabbrörligare. Omvärlden är i ständig förändring. Våra kunder och deras behov förändras hela tiden. Det tycker vi är underbart, eftersom vi då kontinuerligt får möjlighet att lära oss nya saker. Jag har tagit till mig devisen "– Allt som inte är under utveckling är under avveckling" från min mentor Christer Olsson.

Av samma skäl har vi organiserat om oss för att få mer resurser till vårt informations-säkerhetsarbete, där det är många kunder som önskar vårt stöd, liksom till utveckling av efterfrågade tjänster.

Tripnet är ett tillsammans-projekt

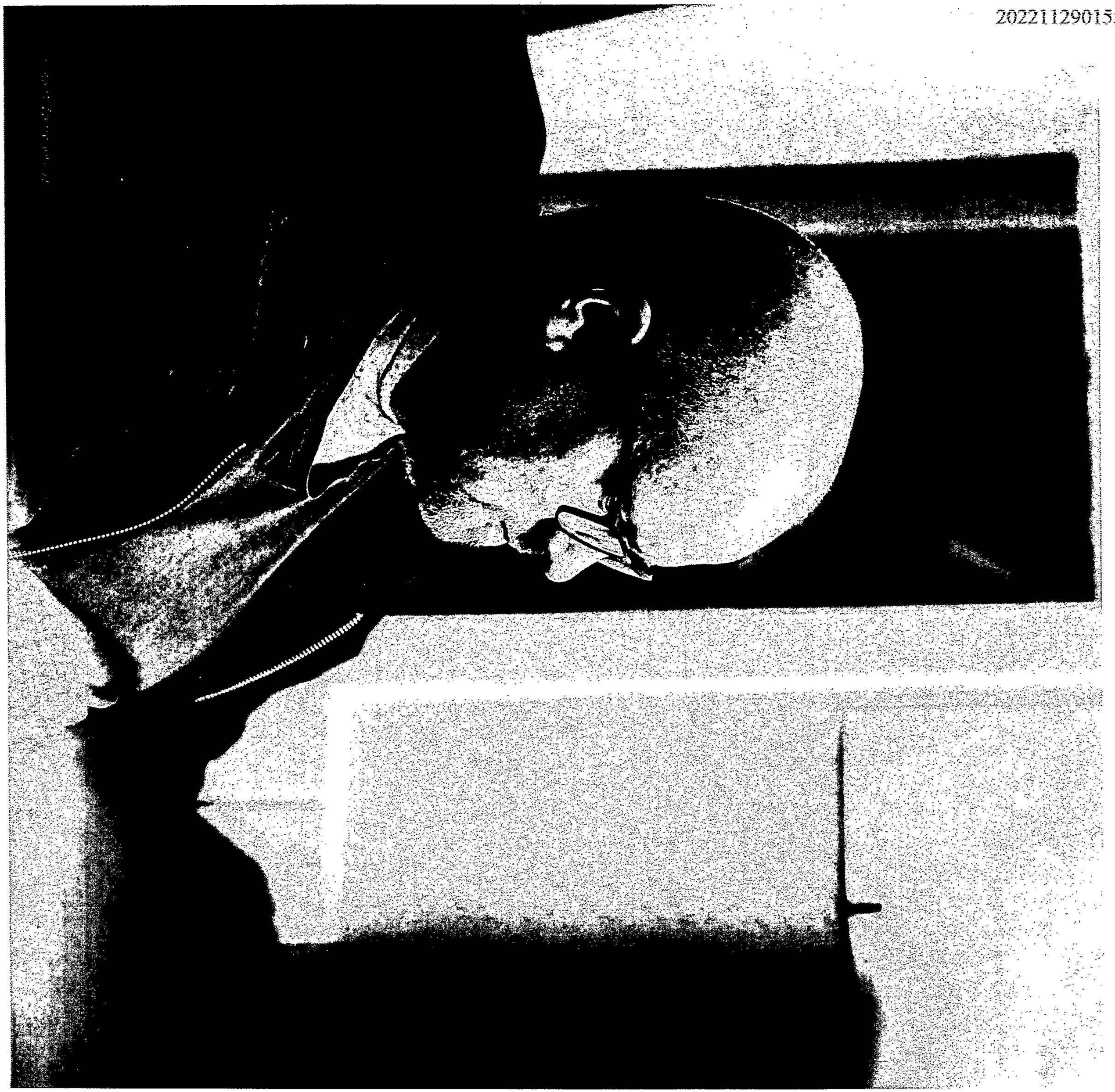
Tripnet är ett på riktigt värderingsstyrt företag. Därför skapar vi våra strategier och vår taktik tillsammans, genom dialog med alla i hela bolaget. Alla på bolaget träffar våra kunder, vilket innebär att alla har tankar om vad kunderna behöver men från vitt skilda perspektiv. När vi gemensamt arbetar fram våra strategier är det min uppgift att leda arbetet, se till att alla kommer till tals och att vi tar vara på alla goda idéer och tankar. Ett sådant arbete brukar bli bra om man låter det ta 12–18 månader för att därefter landa i en gemensam plan som gör att man kan fatta snabba beslut, av alla storlekar och på alla nivåer i företaget. Vår senaste strategi blev klar våren 2021.

Nördarnas paradis

Vi arbetar aktivt med att Tripnet ska upplevas som en attraktiv och värdefull arbetsgivare för nuvarande och framtida medarbetare. Att alla ska uppleva en stimulerande arbetsplats med fokus på välmående, utveckling och delaktighet. Vi skapar detta genom att vi alla på Tripnet är duktiga på vad vi gör, känner möjlighet till självbestämmande och att vi bidrar till ett härligt gäng med nördar av alla slag. Jag är övertygad om att du märker av detta när du träffar oss.

Varma hälsningar,

Ulf Persson
VD och medgrundare



20221129013559

En natt på Tripnet

Varför pratar vi inte mer öppet om informationssäkerhets-incidenter? Visst har vi hört talas om att Kalix kommun drabbades av en ransomware-attack och när Coop fick stänga hundratals butiker på grund av IT-attacken mot Kaseya?

Men, varför är det tyst om dataintrång som gått obemärkt förbi? Är det bara vi som upplever en tystnadskultur? Hur skall vi kunna stötta varandra och utbyta erfarenheter om vi inte utbyter information och kunskap? Nu är ett bra tillfälle att ändra på detta.

Vi på Tripnet och våra kunder utsätts hela tiden för försök till dataintrång. Den absoluta merparten stoppas och passerar obemärkt förbi, men ibland kommer en attack igenom och orsakar incidenter. Den vanligaste anledningen är dåligt underhållna system, oftast gamla applikationer med sårbarheter. Det är väldigt ovanligt med dataläckage och hittills har – ta i trä – ingen av våra kunder råkat ut för ransomware och fått sin data krypterad.

Den allvarligaste incident vi på Tripnet har drabbats av, skedde strax innan klockan 22 en måndag i maj 2022. Vår systemingenjör på plats fick larm och upptäckte hög belastning i en av de VMware-miljöer där vi producerar våra molntjänster. Samtidigt hade två kollegor precis gjort en säkerhetscanning av våra system. Första tanken hos dem var – vad har vi gjort nu? Det var några svettiga minuter för dem innan de fick konstaterat att det inte var de själva som överlastade vår miljö.

Tydlig incidentprocess och transparent kommunikation

Vid störningar arbetar systemingenjörerna enligt vår incident-process, viket är en av våra viktigaste processer. När man har en incident är det väldigt lätt att ryckas med i felsökning och att vilja att lösa problemet. Det känns naturligt, men innebär att man tappar överblicken. Erfarenhetsmässigt tar det max 30 minuter innan man drabbas av tunnelseende. Processen är därför vårt viktigaste stöd för att strukturera arbetet. En av de första sakerna vi gör att är att kommunicera till berörda kunder att vi har en incident, och då hellre till för många kunder än att vi riskerar att missa någon. I detta fall informerar vi samtliga kunder efter 14 minuter från första larm.

Det ger oss möjlighet att koordinera vår felsökning med berörda kunder.

Tillbaka till måndagen i maj. Direkt efter första information skickats, eskalerade ansvarig systemingenjör incidenten. Ytterligare kollegor och vår tekniska chef kallades in. Vid

20221129015600

större incidenter är det mycket som görs på kort tid. Att felsöka, prata med kunder och skicka ut information kräver ett flertal personer.

Vi upptäckte att källan till den höga lasten var ett krypto-miningprogram. Detta program stjäl beräkningskraft för att utvinna kryptovalutan Monero. I samband med detta öppnade vi en säkerhetsincident och ärendet eskalerades till vår säkerhetschef. Vi identifierade en webbhotellserver som källa till spridningen. Eftersom det var akut, togs beslutet att stänga ner denna server, som hanterar en handfull kunder, och kommunicera med dessa. I detta läge ville vi minimera skadan och risken för dataförlust eller -läckage. Senare satte vi upp nya servers för dessa kunder. Dessa servers var, som det heter på bransch-språk, "totally hacked".

På webbhotellservern var angripare inloggade, men de kom aldrig vidare till några andra servers. Dock lyckades de genom ett fel i Microsoft AD skicka vidare illvillig kod. Vi identifierade tidigt ett antal platser på Internet som den illvilliga angriparen kommunicerade med. Vi blockerade dessa för att stoppa spridning, eftersom det fanns script som automatiskt laddade mining-mjukvaran på nytt.

Forensiska analyser och externa specialister

Efter att vi identifierat och isolerat den hackade servern fortsatte vi med forensisk analys för att hitta hur den illvilliga koden tagit sig in och spridits. Parallellt med detta arbetade vi med att analysera om någon data läckt. Denna analys sker i flera etapper. Efter fem intensiva timmar stängs den incident som gäller den höga belastningen, medan säkerhetsincidenten kvarstår och arbetet med de påverkade systemen fortsätter. Eftersom vi snabbt stängde ner angriparnas kommunikation stoppades fortsatta attacker.

Vi konstaterade även att ingen kunddata läckt, men vi såg lokala lösenord på webbhotellservern som röjda. Därför uppmanade vi kunder att byta dessa lösenord om de använt dessa på andra ställen.

Vi insåg tidigt att säkerhetsincidenten var stor och skulle kräva stora resurser för analys, efter att det initiala arbetet var klart. Vi hade kontakt mer flera externa partners för att bolla våra tankar. På grund av arbetets omfattning valde vi dock snabbt att plocka in externa specialister från vår partner Orange Cyber Defence. Insatsen var intensiv och bedrevs tidvis dygnet runt tillsammans med Orange.

För oss är denna incident dessbättre unik. Vi fick en bekräftelse på att våra processer och vår kompetens även fungerade vid en så här pass omfattande incident och att vi har rätt partners. Det är även i sammanhanget bra att ha en extern, tredje part med sig tidigt i processen. Det gav oss information och rapporter från en oberoende part att förmedla till kunder och till deras slutkunder och andra intressenter.

Polisanmälan av cyberbrott

Hur fungerar det att polisanmäla denna typ av brott? Hur gör man och hur agerar polisen? Vår VD Ulf Persson skrev ihop en polisanmälan utifrån vår mall som han tog med sig och åkte till Polisen. När han kom in på Polisstationen på Stampgatan i Göteborg fick han snabbt lämna in sin anmälan i luckan och blev ombedd att vänta kvar. Efter en halvtimme fick han prata med polisen Pernilla. De gick gemensamt

Fredrik Nordlund

20221129015G2

igenom anmälan och säkerställde att alla uppgifter fanns med, och att hon uppfattade informationen rätt. Hon informerade även om hur hon skulle hantera anmälan vidare.

Senare på dagen ringde en annan polis, Thomas, som arbetar med cyberbrott. Han berättade att de såg detta som ett grovt dataintrång och skulle hantera brottet på sin regionala cyberbrottsavdelning. De bad även om kompletterande information. Vi skickade analysen från Orange till dem. Senare kontaktade de oss för att få mer data och kunna göra en fortsatt forensisk analys. Som vi förstår det, var detta ytterligare *en pusselbit i ett större pussel. "Kända gärningsmän", sa de* någon gång.

– Min uppfattning är att Polisen tagit detta på allvar, att de är både professionella och kompetenta att hantera denna typ av brott. Jag tror att denna typ av brottslighet är väldigt svår att utreda, säger VD Ulf Persson. Polisen har klart överträffat min förväntan, jag hade nog inte trott att då se så stort intresse från dem. För mig känns det viktigt att kunna prata om detta och ge polisen den hjälp de behöver. De har sannolikt en helt annan övergripande bild än vad vi har.

Slutsatser

För att ens kunna hantera dataintrång är det avgörande att man kan upptäcka dem. Givetvis ska man ha många skyddslager runt sina system, men man kan inte längre lita på att det alltid räcker med smarta brandväggar och nästa generations antivirus. Man behöver räkna med att systemen inte bara blir utsatta för försök till dataintrång, utan även att dessa kan lyckas. I samband med incidenten installerades ytterligare mjukvaror på servrarna för att hjälpa oss i den forensiska analysen och för att säkerställa att inte illvillig kod kan startas och om den ändå skulle startas – att vi upptäcker den.

Snittiden det tar att upptäcka ett dataintrång är 287 dagar. Det räcker inte år 2022! Se sida 20. I denna incident kunde vi både upptäcka och agera snabbt. Ofta har man lite tid på sig, men ju fortare man agerar, desto bättre. Det är viktigt att planera för vad som är viktigt, tänka på tillgänglighet, konfidentialitet och integritet. I vilket läge ska systemen plockas bort från Internet och vad krävs för att återansluta dem igen?

Efter incidenten har vi funderat lite kring om det är hotbilden eller kravbilden som har ändrats?

– Jag tror att det i takt med att en ökad andel av intäkterna genereras genom IT, kommer det automatiskt förväntningar om hög tillgänglighet, helst 100 %, säger Ulf Persson. Det är numera självklart att affärs- och samhällskritiska system kan publicera på Internet och då skall de även vara 100% konfidentiella, så kravbilden har ökat. Det pågår i skrivande stund ett krig i Europa och det är stora spänningar i vår omvärld, så hotbilden har också ökat.

20221129015G3

TIPS FRÅN OSS PÅ TRIPNET

• Skydda dina system i många lager. Funktioner som skall förhindra intrång, t ex antivirustjänster behöver övervakas.

• Förutsätt att dataintrång kan ske, oavsett dessa lager.

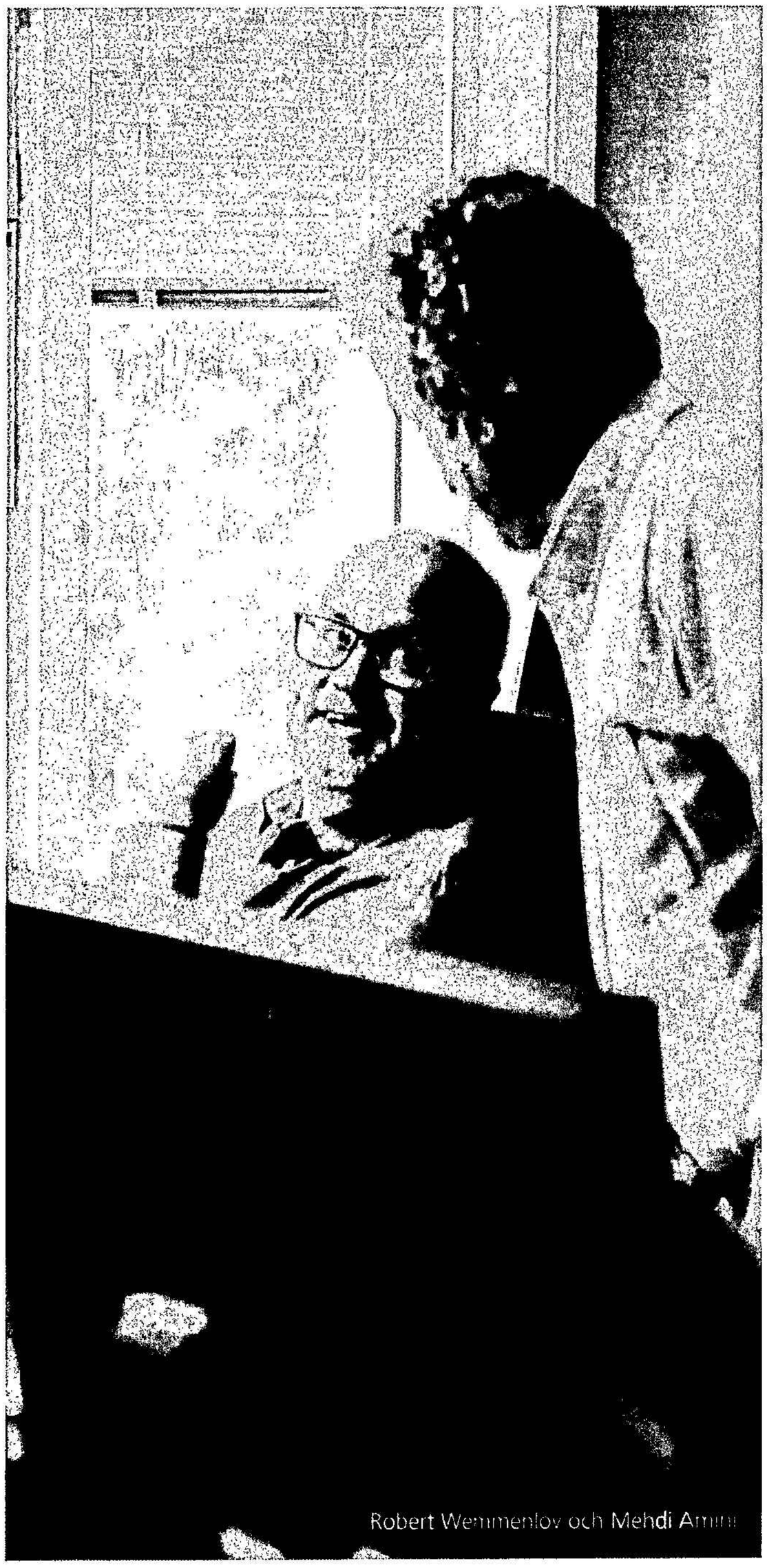
• Programvara för detektering och åtgärd av illvilliga operationer (EDR) behövs och ska övervakas.

• Planera i förväg. Fundera inte på om du kommer att bli hackad, utan när. Säkerställ att du har tillgång till experter och resurser om det skulle behövas.

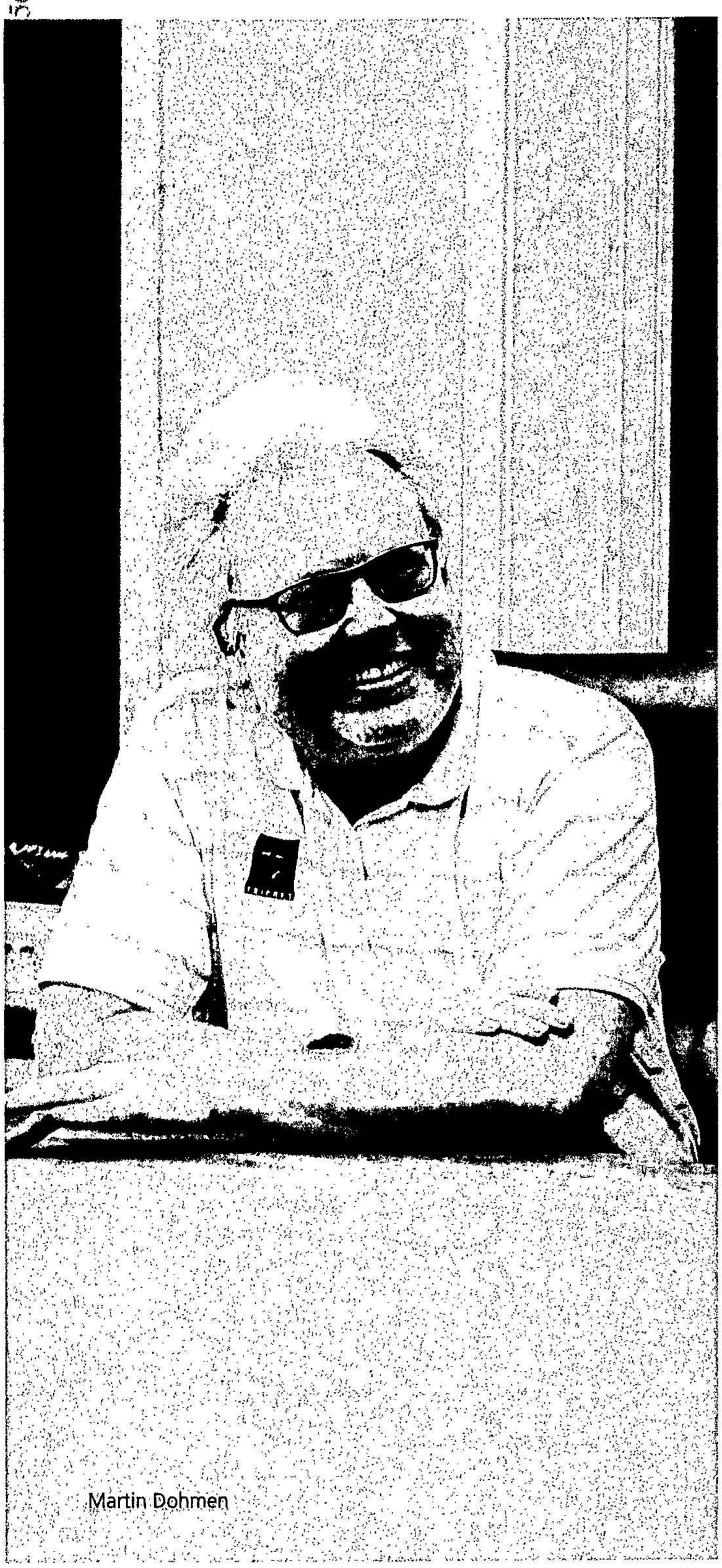
• Arbeta strukturerat med informationssäkerhet

Då har du koll på dina informationstillgångar och kan fatta välgrundade beslut.

Marcelo Cáceres Longé



Robert Wennmenlov och Mehdi Amini



Martin Dohmen

1994 – då säkerhetsfrågan var obefintlig

Idag kretsar en hel del av arbetet här på Tripnet runt hur vi på bästa sätt upprätthåller säkerheten på de system som vi har driftansvaret för. Det har dock inte alltid varit så...

Följ med mig på en historisk resa och mina minnen från de första åren – från att tankarna på att starta en verksamhet började ta form 1994 till hur vi sedan kom i gång med vår modempool året därpå till att sedan utveckla webbhotells-tjänster de kommande åren.

Från riks till lokalt

En av våra drivkrafter bakom att starta Tripnet var väldigt enkel. Det fanns inte någon lokal ISP i Göteborg vilket gjorde att man med uppringd internet betalade för "rikssamtal" till Stockholm. Priset var över en krona i minuten, vilket snabbt blev kostsamt om man ville vara uppkopplad en längre stund. Detta gjorde att vårt fokus i början handlade om att etablera en modempool i 031-området för att slippa betala höga minutavgifter till Telia, som förresten precis hade bytt namn ifrån Televerket.

20221129015657

Direkt från start använde Tripnet Linux, vilket då var nästan nytt. Internetservrar kördes vanligen på någon av de stora Unix-dialekterna som Solars från SUN, då dessa hade en stark ställning bland världens universitet och stod för en stor del av internetanvändandet. Att Tripnet valde Linux berodde på att en av grundarna hade experimenterat en del med Linux och hade insett hur prisvärd en standard-PC med Linux var, jämfört med en SUN med Solaris som han arbetade med till vardags.

Fokus på tillgänglighet och stabilitet

Den första tiden låg fokus på tillgänglighet och stabilitet, då allt inte var helt moget. Vi brottades med allt ifrån modem som blev opålitliga så fort de varit på några dagar till serieportsdrivrutiner med buggar som bara dök upp när man hade många serieportar i samma server. Detta ihop med att utvecklingen gick snabbt på Linux gjorde att vi ibland uppdaterade våra servrar dagligen i jakt på den senaste buggfixen som skulle lösa något av våra stabilitetsproblem.

Att lägga på patchar på sitt operativsystem var dessutom ett ganska stort äventyr jämfört med idag. På Linux-sidan var det normala förfarandet att kompilera sin egen kernel, och då laddade man inte ner hela källkoden på nytt eftersom den var stor och det tog lång tid, utan man utgick ifrån den version man redan hade och laddade bara ner patcharna, så kallade diff-filer, innan man kompilerade kerneln på nytt. Detta tog inte bara lång tid, det var också mer regel än undantag att något gick fel i hela processen och man fick börja från början. Även när man kommit hela vägen och installerat den nya kärnan var det fortfarande bäst att hålla tummarna för att den verkligen skulle boota. Att vi dessutom använde relativt ovanliga serieportkort i våra Linux-servrar för att kunna ansluta 24-modem till varje server, gjorde att vi drabbades av en del tidigare oupptäckta fel i Linux serieportsdrivrutin.

Starkt stöd av ikoniske Alan Cox

För att få bukt med dessa fick vi hjälp Alan Cox som på den tiden var Linus Torvalds högra hand när det gällde utvecklingen av Linux. Han skrev kernel-fixar till oss men eftersom han inte hade den hårdvara vi använde, och vi själva inte hade några test- eller labb-servrar med denna hårdvara, hade dessa fixar inte testats alls innan vi körde dem i vår produktion. Kanske inte helt konstigt att både jag och Daniel Ryde, som var de två som mest jobbade med tekniken på Tripnet, lade oss till med vanan att ringa vår modempool varje gång vi hade varit i närheten av Tripnet och skulle åka hem. Det var lika jobbigt varje gång man kom hem och behövde vända i dörren för att något hade hängt sig! Tilläggas ska att ingen jobbade heltid på Tripnet. Vi hade inte heller något övervakningsverktyg som

20221129013566

kunde larma när något var sönder utan fick förlita oss på att både vi själva och våra vänner och bekanta använde tjänsterna och ringde oss när något var trasigt.

Tripnet öppnade ett av Sveriges första webbhotell

I våra modemabonnemang ingick möjligheten att ladda upp en egen hemsida men den hamnade då på en adress som tillhörde Tripnet som kunden inte kunde påverka. Ganska snart började det dyka upp förfrågningar om att kunna ha webbsidor på kundens eget domännamn, vilket inte var helt enkelt att lösa. Varken http-protokollet eller den webbserver-mjukvara som var dominerande, NCSA HTTPd, var gjorda för att hantera flera olika domännamn på samma server. Detta var långt före de virtuella servrarna så normalt krävdes en dedikerad fysisk server för varje domännamn. Med en del arbete, pålagda patchar och andra workarounds lyckades vi faktiskt skapa ett av Sveriges första webbhotell där du fick eget domännamn och där det inte syntes i adressfältet i browsern att du delade server med andra kunder.

Men säkerheten då?

Nästan inga av de verktyg som idag är helt självklara och oundvikliga – i alla fall inte om du vill ha en Internetansluten server – användes och vissa av dem fanns inte ens ännu. Varken brandväggar, antivirus, kryptering eller 2FA var vanligt använda för Internetservrar. Vi använde inte heller VLAN, utan alla datorer, oavsett om de var webbservrar, klientdatorer eller Novell-filservern, satt på ett och samma nät som var direktanslutet till routern från vår Internetleverantör. Nätet var ett 10Mbit/s coax ethernet, Internetanslutningen var 64Kbit/s och WiFi var inte uppfunnet ännu. Novell-servern hade gissningsvis inte ens TCP/IP installerat, klientdatorerna kördes på Windows 3.11 och Trumpet Winsock.

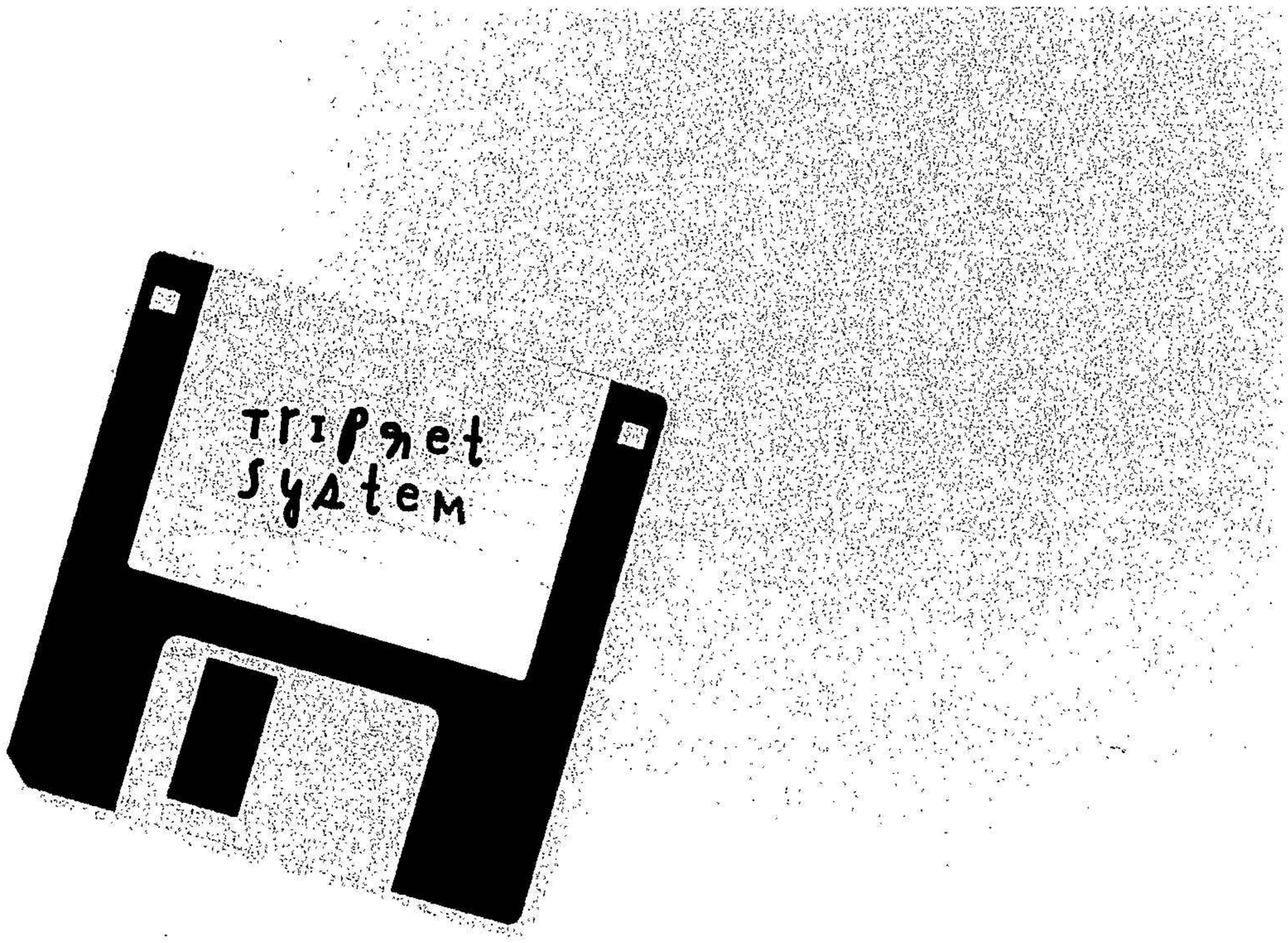
Microsoft släppte inte ens en egen IP-stack förrän i Windows 95.

De säkerhetsåtgärder vi jobbade mest med var att "härda" operativsystemen, dvs stänga ned onödiga tjänster som var i gång som standard. En del av dem krävde inte ens inloggning för att kunna användas – eller missbrukas. En av anledningarna till att detta precis börjat ses som viktigt var att ett av de första sårbarhetsscanningsverktygen, SATAN, precis hade släppts. SATAN eller "Security Administrator Tool for Analyzing Networks" som det egentligen hette men ingen någonsin kallade det, fick ganska stor uppmärksamhet då det dramatiskt förenklade arbetet med att skanna efter sårbara tjänster på ett nätverk och användes av hackare med både vita och svarta hattar. En del var av uppfattningen att det var oetiskt att släppa ett så här farligt verktyg fritt på internet men i efterhand så är det för mig ganska tydligt att det snarare satte fokus på att det var viktigt med säkerhet. Flera av de stora tillverkarna, såsom HP, Sun och IBM, kom som ett direkt svar på SATAN ut med bulletiner om vad systemadministratörer behövde göra för att säkra deras produkter – information som tidigare varit mycket svårare att hitta.

Kryptering var fortfarande i sin linda. Utvecklingen av funktioner som vi idag tar för givna, såsom SSH och HTTPS, pågick men var mer eller mindre oanvända, ofta av bra skäl. Till exempel blev HTTPS inte standard förrän år 2000 och innan dess var det inte säkert att en webbläsare från en tillverkare kunde prata med en webbserver från en annan om man försökte använda kryptering.

Eftersom kryptering inte användes var det fortfarande väldigt vanligt att lösenord skickades runt i klartext, vilket ju självklart var en säkerhetsutmaning. Fick man in någon typ av malware

20221129013567



på en dator var en av de första saker den försökte göra att avlyssna nätet efter lösenord, och utan nätverkssegmentering, och inte ens några switchar, kunde alla datorer på ett nät avlyssna all trafik och lätt komma över alla lösenord som användes i nätet. Därför pågick ett arbete att byta till protokoll som åtminstone inte skickade lösenordet i klartext, till exempel var CHAP helt nytt och ansågs mycket säkrare än PAP som ersattes.

Säkerhetsarbetet påbörjades – och pågår fortfarande

Efter några år började 1995 års statiska webbsidor ersättas med mer avancerade webapplikationer, skrivna i språk som PHP, Java och ASP. Ungefär samtidigt började Microsoft få fotfäste på webbservermarknaden med NT4 och IIS. Webbshoppar började dyka upp och med dem ökade insikten om behov av säkerhet runt systemen, även om det fortfarande då var ganska många år kvar till att kortindustrin skulle ta fram sin säkerhetsstandard PCI. Kombinationen av mer komplicerade system och högre krav gjorde att säkerhetsarbetet började rullas framåt, och vad jag kan se så rullar det fortfarande.

Vi på Tripnet fortsätter där vi började. Med förbättringsarbete och ökad användarnytta i fokus. Då kanske främst för att spara pengar och för att teknik var galet kul – idag mer för att skydda och värna om våra kunders värdefulla data. Och för att teknik är galet kul!

Martin Dohmen
Medgrundare och Solutions Director

20221129013568

Skydda företaget från en cyberattack

Kanske är det först när man drabbas av en cyberattack som man förstår vilka risker man utsatt sig för? Alla företag som inte vill drabbas framöver behöver därför vara beredda på var hoten finns för att kunna hantera dem. Marcelo Cáceres Longé, ansvarig för informationssäkerheten på Tripnet, guidar oss genom de aktuella hotbilderna – och vad vi kan göra åt dem.

Att påstå att Sverige ligger i framkant när det gäller digitalisering är absolut inte en överdrift. De senaste 20–30 åren har svenska företag investerat stora summor i teknologi och digitalisering, vilket är en stor anledning till att vårt samhälle ser ut som det gör i dag. För Marcelo Cáceres Longé är detta extra tydligt när han jämför Sverige med Spanien, där han har bott i tio år.

– Sist jag skulle byta bil i Spanien tog det mig en hel dag och kostade ungefär 5 000 kronor, i jämförelse med hur jag i Sverige bara kan scanna det gula pappret i Transportstyrelsens-app, betala med Swish och tre minuter senare ha bilnyckeln i handen, berättar Marcelo. Att vårt samhälle är så pass digitaliserat är positivt eftersom det har förenklat vår vardag, men digitaliseringen har också medfört kompromisser med säkerheten och gjort oss mer sårbara. Om någon app, något företag eller någon
myndighet blir utsatt för en attack så har det stora konsekvenser och kan göra oss mer eller mindre handlingsförlamade. Enligt en rapport av säkerhetsföretaget Truesec får 76 procent av de framgångsrika cyberattackerna fotfäste i en IT-miljö på under två timmar och det tar oss sedan ungefär 287 dagar att upptäcka, identifiera och agera på attacken.

Digital affärsrisk

För att kunna bemöta hot behöver företag en tydlig säkerhetsstrategi med en plan för hur man:

1. Identifierar risker.
2. Analyserar och värderar risker.
3. Bestämmer om risken ska accepteras eller åtgärdas.
4. Hur uppföljningen ska gå till.

Det är viktigt att det finns en tydlig beskrivning för hur man återhämtar sig efter till exempel en cyberattack, eftersom det annars är lätt att agera i affekt.

20221129015 70

17 % av svenska företag är helt omogna
I Sverige är ca 17 procent av företagen helt omogna att hantera cyberattacker. Dessa upplever inte digitaliseringen som ett problem och ser istället säkerhet som ett stort hinder för verksamheten. Det är endast en låg andel av investeringarna som läggs på säkerhet.

31 % av svenska företag är på basnivå
Inte heller dessa företag ser digitaliseringen som ett stort problem för säkerhet, men till skillnad från tidigare nämnda så prioriteras både digitalisering och innovation relativt högt. Även dessa företag på basnivå lägger endast en låg andel av investeringarna på säkerhet.

27 % av svenska företag är kvalificerade
För att företaget ska räknas som kvalificerat ska digitalisering och innovation prioriteras högt, även om företaget inte ser digitaliseringen som ett problem för säkerheten. Av de totala IT-kostnaderna ska tio procent investeras i säkerhet, som till exempel brandväggar eller antivirussystem. Dessa företag inkluderar även säkerhet som en parameter i sina kundnöjdhetsfrågor.

26 % av svenska företag är förberedda på att hantera cyberattacker
Företag som är mogna i att hantera cyberattacker kännetecknas av att de insett att ökad digitalisering är ett problem för säkerhet och prioriterar därför inte att ligga i framkant gällande teknik och digitalisering. Fler än tio procent av de totala IT-kostnaderna investeras därför i säkerhet. Säkerhet är också en parameter som alltid inkluderas i kundnöjdhetsfrågor.

– Under mina år på Tripnet har jag lärt mig att säkerhet är något man aldrig kan bli klar med. Säkerhet är ett kontinuerligt arbete som alltid måste fortsätta, konstaterar Marcelo Cáceres Longé.

Identifiera och hantera beroenden
För de flesta av oss är det väldigt svårt att bedöma om komponenterna i en server i eller dator är säkra genom att titta på dem, och det är nästan omöjligt att knäcka koder för att bedöma om mjukvaran är säker. Det är därför inte ovanligt att välja andra strategier för att bedöma säkerhet. För många är lösningen att köpa produkter och tjänster från välkända företag som uppfattas ha en låg risk, men tyvärr är det inte riktigt så enkelt.

– Även om man väljer en känd och etablerad tillverkare behöver man göra någon typ av säkerhetskontroll. Vid ett tillfälle var vi på Tripnet intresserade av att köpa nätverksutrustning från ett välkänt globalt företag. Då var det enorm tur att vi gjorde en kontroll. När vår professionella partner Radar kollade lite närmare, visade det sig att produkterna inte levde upp till vår önskade säkerhetsnivå, berättar Marcelo Cáceres Longé. När det gäller säkerhet är det alltid bättre att göra en kontroll för mycket, än att göra en för lite. Vi är i dag ytterst tacksamma över att ha experter vid vår sida som hjälper oss att ta viktiga beslut!

Risken med en ny plattform
Molntjänster är idag något de flesta företag använder sig av i någon form, men det är också väldigt problematiskt. Molntjänsterna erbjuder en stor mängd tjänster som användarna inte alltid känner till och det är många människor

20221129015711

som är involverade och inloggade. När företaget flyttar till en ny plattform finns risken att de har felkonfigurationer och blir extra sårbara för cyberattacker - därför är det otroligt viktigt att göra sina säkerhetskontroller vid dessa tillfällen.

– Tidigare, när jag jobbade med pre-sales på Tripnet, var jag med på möten med kunder som ville flytta till en publik molntjänst och jag frågade då alltid vad som triggade kunden att flytta. Åtta av tio gånger var svaret att det var ledningens beslut, beskriver Marcelo. Min slutsats är att företag väljer att byta från en känd plattform till en okänd sådan för att spara pengar, vilket är ett mycket farligt beslut!

Molntjänster är inte dåliga per se, men det är viktigt att alltid be om insiktsfulla råd från professionella människor innan man fattar ett sådant beslut.

Cyberattacker - det ständiga hotet

Den som har en dator och är uppkopplad till internet kan cyberattackera vilket företag som helst, var som helst i världen – enbart genom att betala för det! Attackerna i dag är dessutom mer automatiserade och skräddarsydda. När är det egentligen bäst att attackera ett svenskt företag? Det är inte helt omöjligt att attacken schemaläggs till en fredagskväll, när man precis satt sig i TV-soffan med familjen.

– Som jag tidigare nämnde tar det endast två timmar för en framgångsrik attack att få fotfäste i ett system, så innan filmen är slut är redan hela miljön infekterad, förklarar Marcelo Cáceres Longé. Om vi har tur upptäcker vi det när vi försöker starta datorn på måndagen, men om vi inte har tur tar det oss 287 dagar att upptäcka det... Då kan de cyberkriminella ha använt vår miljö för illegala ändamål i nästan ett helt år.

Utpressningsprogram – ransomeware

När syftet är att pressa företag på pengar används särskilda utpressningsprogram, även kallade ransomware, som kan kryptera alla filer och backuper. För att få tillbaka sin data eller för att hindra känslig information från att läcka, kan företaget tvingas betala stora lösensummor. Om man vill identifiera den här typen av attack i god tid gäller det verkligen att skydda sina system.

Vi är den svaga länken

Oavsett hur avancerade verktyg vi har och vilken säkerhet vi försökt bygga upp i våra system finns det alltid en svag länk i den mänskliga faktorn.

– Det räcker med ett enda felklick för att angriparen ska ha full kontroll över dina system, förtydligar Marcelo.

Så, hur kan vi förbereda oss för den typ av attacker som siktar in sig på en enskild individ? Det viktigaste är att vara medveten om att de finns och att samtliga medarbetare är informerade om hur de ska agera. Att välja ett bra antivirusprogram som kan upptäcka försök till attacker och använda multifaktorsautentisering på alla sina system är också viktiga skyddsåtgärder.

Vem bär ansvaret?

Det är inte helt ovanligt att vilja skylla ifrån sig och avsäga sig ansvaret när attacker faktiskt inträffar, men i ärlighetens namn vet samtliga om att det inte är rätt väg att gå för att lösa problemet. Både leverantören och kunden bär ansvar för att

20221129015T2

förhindra den här typen av attacker. Vi, som är leverantörer av IT och säkerhet, bör bygga upp våra tjänster utifrån just säkerhet, gå i bevis för det samt kontinuerligt revidera våra rutiner och processer. Kundens ansvar är att kräva dessa revideringar.

– Rätt säkerhetsnivå är inte samma sak som 100 procent säkerhet. När jag hör någon prata om 100 procent säkerhet, då vet jag att det inte är seriöst, säger Marcelo. Rätt säkerhetsnivå handlar om att jämföra påverkan och kostnad, och hitta en nivå som är godkänd.

Att skydda sin data

Att kontinuerligt arbeta med säkerhet är fundamentalt för att behålla en hög säkerhetsnivå. Många människor väljer att placera all sin data på samma plats, men det är inte det bästa tillvägagångssättet. Viss data är mer känslig än annan, vilket också gör det logiskt att välja rätt plats till rätt data. När det gäller skydd av identitet och data så är loggning av vad som händer A och O. Om man loggar vem, när och var så kan man sedan lära sig av det som har hänt och på så sätt försöka förhindra framtida attacker.

Arbete på distans - det nya normala

Något som verkligen har blivit vardag för oss efter pandemin är möjligheten att utföra sitt jobb på distans. Bekvämt enligt många, men också något som gör oss sårbara i högre omfattning. De verktyg vi har på kontoren kan övervaka våra lokala nätverk, men de är inte kapabla att övervaka system på andra sidan jorden. Det finns samtidigt även en risk att det sitter någon bakom dig på caféet eller tåget och kikar över axeln.

– Jag minns ett särskilt tillfälle under pandemin då jag jobbade hemifrån och satt i ett Teamsmöte med en kund. Mitt i mötet, när jag ställde en fråga till kunden, så satte min Google Home igång och började svara mig, återberättar Marcelo Cáceres Longé. Detta gav mig verkligen en tankeställare! När jag ska prata om informationssäkerhet med mina kunder är jag sedan den dagen noggrann med att dra ut alla kablar och stänga av telefonen.

Marcelos rekommendationer

- Inventera alla tillgångar i er IT-miljö.
- Gör en säkerhetsbedömning. Vilka innehåller känslig data?
- Skapa en incidenthanteringsplan. Hur ska incidenten lösas och vem gör vad?
- Minska attackytan, till exempel genom att avveckla oanvända datorer.
- Uppdatera systemen och övervaka kritiska system, helst dygnet runt.
- Kontinuerlig information och utbildning minskar risken med den mänskliga faktorn.

20221129015T4

Certifiering som skapar affärsnytta

Ett ämne som engagerar många: ISO27001 – certifiering och revision. Men vad är egentligen ISO27001? Vad finns det för fördelar med att efterleva standarden? Vilka krav ställer ISO27001 på organisationen? Hur går det till att certifiera sig? Tripnets säkerhetschef Göran Sjöberg har tillsammans med Per Gustavsson, CISO på Stratsys AB, hjälpt oss reda ut alla frågetecken och samtidigt bjudit på inspiration, klokhet och insiktsfulla råd.

Säkerhetsfrågor är högaktuella. Anne-Marie Eklund Löwinder rankas som en av Sveriges främsta experter på informationssäkerhet. Hon är en av de fjorton betrodda människorna i världen som har en nyckel till internets hjärta, det vill säga domännamnssystemet DNS. I Sommar i P1 den 27 juli 2022 sa Anne-Marie "DNS är internets vägvisare som guidar oss användare så att vi hamnar där vi tänkt oss eller där vi tror att vi är".

– Det blir så tydligt för mig att ISO 27001 handlar om just tilltro till att all den information som vi både skickar och läser på nätet faktiskt är korrekt och säker, konstaterar Göran. Anne-Marie pratade om ceremonier, processer, rutiner och kontrollfunktioner och allt detta, tillsammans med olika tekniska säkerhetslösningar, är faktiskt det som tillsammans bygger vår tillit till den informationen vi får. Enligt en tidigare studie av Radar är det bara hälften av alla verksamheter som anser att säkerhet är viktigt! Det är ju skrämmande, säger Göran.

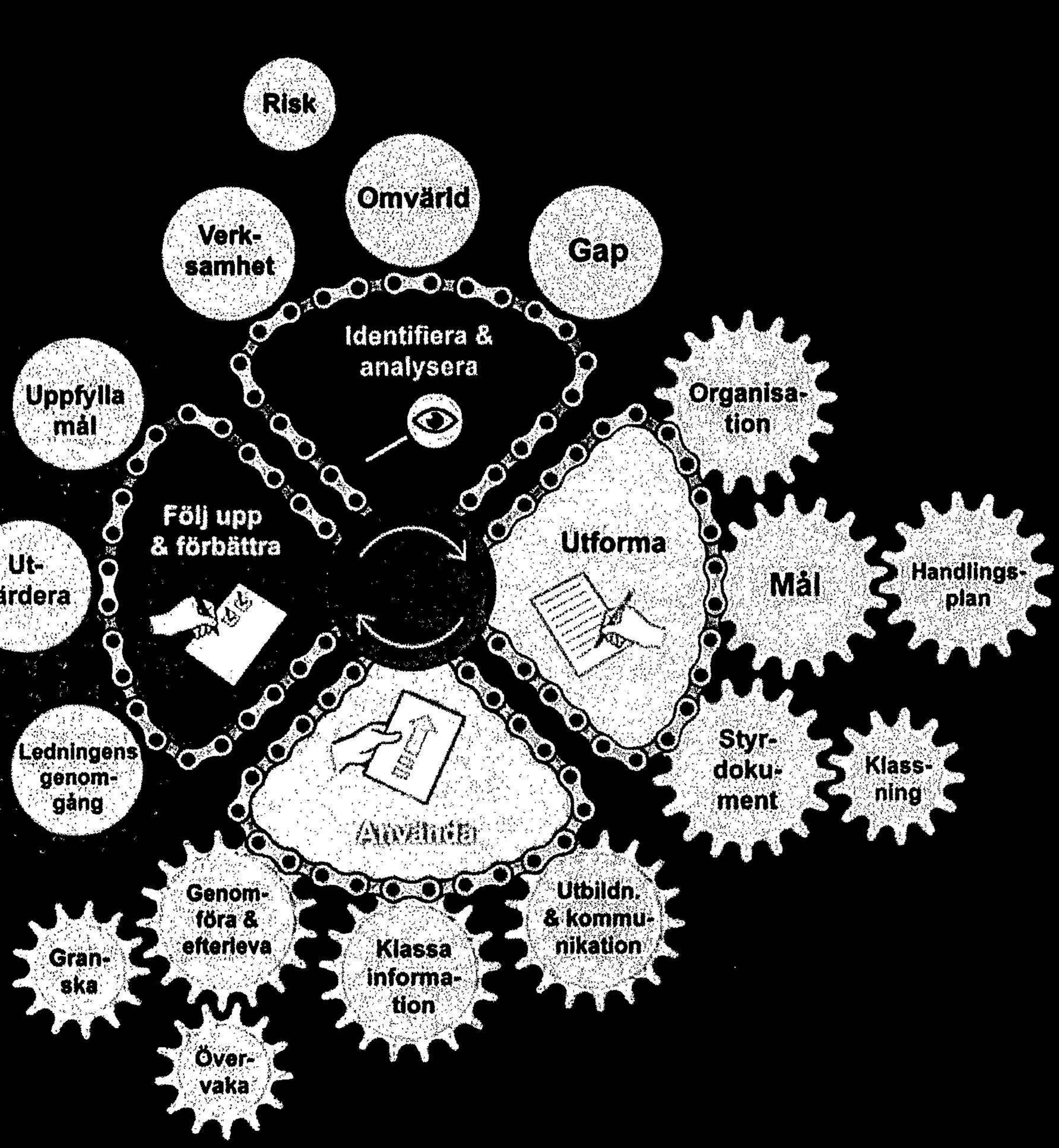
Standarder i ISO 27000-serien är framtagna på att skydda information och omfattar också cybersäkerhet och dataskydd. Här ingår ISO 27001 som är en standard med specifika krav för att upprätta, införa, underhålla och hela tiden förbättra din informations- och cybersäkerhet. Standarden innehåller generiska krav och passar alla organisationer, oavsett storlek eller bransch, men är främst riktad till de som hanterar känslig eller stora mängder information.

– När vi pratar om ISO 27001 pratar man tyvärr ofta om olika saker. Det är 27001 som är grunden och kravställaren för att uppfylla standarden. Sedan finns det i 27000-serien även mängder med guider och dokument, exempelvis 27701 som handlar om personlig identifierbar information och 27005 som berör risk management, berättar Per Gustavsson.

– Ofta misstar man sig och tror att dessa guidelines är tvingande. Så är det inte. Men – det är åtgärder man BÖR göra, betonar Per. Man kan se dem som bilagor med väg-

375

VILKA KRAV STÄLLER ISO 27001 PÅ DIN ORGANISATION?



20221129015776

ledning men i slutändan väljer man själv precis vilka säkerhetsåtgärder man vill vidta, förklarar Per. Däremot kan det vara en fördel att följa rekommendationerna, eftersom det då blir lättare för en extern auditor att jämföra. Det enda som spelar roll är att man kan visa att man lever upp till de sju kravgrupperna i kapitel 4 till 10, förklarar Per.

ISO 27001 ger idel fördelar

För tio år sedan var det ingen som pratade om säkerhetscertifieringar. För fem år sedan började det bli "nice-to-have". I dag är det ett krav att kunna visa sina kunder att verksamheten håller hög kvalitet, även på detta område.

Proaktivt skydd för dina affärshemligheter och information är en given fördel, liksom vinsten i att ha ett effektivt ledningssystem för att kontinuerligt och systematiskt hantera incidenter, händelser och ständig förbättring.

– Det är ju kraven som certifieringsorganet ställer på oss för att vi ska få vårt certifikat, säger Göran. Vi jobbar med riskbaserade säkerhetsåtgärder, det vill säga vi identifierar risker i vår verksamhet och sen beslutar vi oss för vilka åtgärder vi ska sätta in. Därmed har vi också bra kontroll över vilka investeringar vi måste göra i teknik. Kostnadseffektivitet, helt enkelt.

ISO 27001 ställer krav på organisationen

I organisationen behöver vissa processer finnas på plats. Det krävs att man analyserar och identifierar exempelvis omvärldsrisker och gap, sett ur ett informationssäkerhetsperspektiv. Därefter måste man utforma hur organisationen ska se ut, vilka mål man arbetar mot, handlingsplaner, styrdokument osv. Själva användandet handlar om att få organisationen att utbilda, kommunicera, genomföra, granska och övervaka. Slutligen uppföljning och förbättring, vilket är grund och syfte i certifieringar generellt.

Certifiering – steg för steg mot målet

Certifieringsarbetet börjar med planeringsdialog som innebär att certifieringsorganet förbereder sig, läser in sig på befintlig dokumentation och ledningssystem för att förstå vad det är de ska revidera.

– Man bör göra en förrevision, föreslår Göran. Den kan antingen göras helt internt eller så tar man hjälp av någon från utsidan. Detta är ett trevligt sätt att förbereda sig inför certifieringsrevisionen. I denna framkommer eventuella avvikelser som man ges chans att arbeta med och korrigera. Sen kommer det efterlängtade cerifikatet, säger Göran och ler. Då kan man direkt börja nyttja de affärsmässiga fördelarna; göra bättre och fler affärer!

Certifieringen handlar om ständig förbättring, vilket innebär att årliga revisioner leder fram till omcertifiering, som görs vart tredje år.

– Låt mig berätta om ett exempel. Den verksamhet jag arbetar med just nu har vuxit så det knakat på sistone, så att inte döda kreativiteten med nödvändiga organisationsförändringar är jätteviktig. Här vill man ju att det rätta valet ska vara det lätta, berättar Per.

För att kartlägga organisationens förutsättningar finns det en del punkter att gå igenom och bocka av:

20221129015T7

- Organisationens förutsättningar
- Ledarskap
- Planering
- Stöd
- Verksamhet
- Utvärdering av prestanda
- Förbättringar

– Att förstå verksamheten, hur de tjänar pengar, var de finns och, kanske ännu viktigare, få svar på frågan om ledningen, styrelsen och ägarna verkligen vill genomföra processen, är avgörande, menar Per. Det är också planeringen. Vi behöver enas om det är hela eller delar av verksamheten som ska certifieras. En annan avgörande faktor är utvärdering av ledningssystemet. Slutligen förbättringar, som återigen är kopplade till ledningssystemet; det man identifierat som är i behov av förbättring och kontroll, beskriver Per.

Arbetet startar i ledningen

Ledningens insikt och ambition är A och O för framgångsrik certifiering. Processen måste också vara anpassad utifrån organisationens förutsättningar. Det gäller att ta hänsyn till interna processer och påverkande aspekter.

– Värt att tänka på är att denna standard är framtagen med utgångspunkten att det finns ett fysiskt kontor, men pandemin har ändrat på spelreglerna, säger Per. Vi sitter utspridda på många olika orter runt om i Sverige och grannländerna så för att slippa ta hänsyn till exempelvis norsk lagstiftning har vi valt att hantera allt utanför oss som om det var utanför Sverige. Dit hör tydligen också Skövde, där jag sitter, säger Per på sjungande västgötska.

När det kommer till planering är det nödvändigt att förstå hur certifieringen är nyttig för verksamheten. Hur ger den något tillbaka? Hur räknar men hem investeringen? Att definiera målsättningar stöder processen och gör att man vet med större säkerhet att man gör rätt saker. Hur tar man då detta till att bli informationssäkerhet och dataskydd?

– Informationssäkerhet och dataskydd har bara en funktion enligt min mening och det är att skapa en lagom nivå av säkerhet, precis på gränsen, till minsta möjliga kostnad, intygar Per. Det är inget problem att bygga ett kärnkraftverk i den här processen men det är inte det som är målet. Vi vill säkerställa våra kunders krav på säkerhet, kvalitetssäkra produktutvecklingen och rakryggat kunna stå upp och svara att "jo, men vi har plockat in en extern granskare som har tittat på oss och som säger att vi följer de processer vi har utlovat". Målet är det kvitto som certifieringen gav oss. Därför gillar jag oanmälda inspektioner! De dyker upp när vi är som sämst, när vi är oförberedda. Om vi då lever upp till kraven – då är vi bra!

Identifiera och fokusera på det som är mest affärskritiskt

För att identifiera de mest kritiska affärsprocesserna kan en workshop vara ett användbart verktyg.

– I vårt fall var det uppenbart att den största och direkt livshotande risken var ett eventuellt stillestånd, konstaterar Per. Vi skulle inte överleva att ligga nere två veckor. Med den insikten blev Tripnets kvalitet avgörande för oss. Jag minns att vi vid leverantörskontrollen till och med tittade hur mycket diesel som fanns i reservaggregatet, berättar Per.

20221129013778

När jag kunde få ett transparent svar på hur länge Tripnet skulle hålla ut under ett strömavbrott kunde vi unna oss att vara helt lugna. Och att med egna ögon få se kapaciteten är häftigt. Hur många har klappat ett dieselaggregat på Amazon eller Microsoft, skojar Per.

Alla måste dra sitt strå till stacken

Utifrån den mest affärskritiska processen kan man sedan, om man vill, förfina och hitta andra delar att kvalitetssäkra och certifiera, men det gäller att det finns resurser över tid. Det är också viktigt att involvera samtliga i organisationen. Alla medarbetare måste bidra på sitt område i arbetet.

– I mitt exempel identifierade vi den överhängande affärsrisken i ett eventuellt stillestånd, men alla i organisationen behöver viss kompetens inom informationssäkerhet. Ta HR, till exempel. Vilka risker utsätter de sig för varje dag? Med rätt kunskap kommer de själva att hitta just sina risker och kan då få hjälp att facilitera, beskriver Per. Delaktigheten sitter i att det inte ska vara management som styr utan de som i vardagen annars bär smärtan, även om det inte är de som är de egentliga riskägarna.

En smidig lösning på internrevisioner är helt enkelt att göra en checklista. Beskriv den beslutade processen, låt någon kontrollera att den följs och om så inte är fallet, då läggs avvikelsen in i systemet. Det är mycket bättre att de som vet hur det fungerar gör auditen. Då gynnas delaktigheten och synergivinsten blir lärande om processerna där det gör nytta.

– Avvikelser är guld för förbättringsarbetet, tycker Per. Avvikelserna hjälper ju till, inte bara att hitta det som gäller informationssäkerhet utan det stöttar hela organisationens kvalitetsförbättringsarbete.

Det finns en stor vinst i att gå en certifieringskurs för att få en känsla för alla de här delarna som man måste kunna – men också för att veta var man kan gena. Oavsett är valet av tidpunkt att påbörja certifieringsarbetet steg nummer ett.

– Det första du måste göra är att inse att det är bara att göra det! I och med att vi faktiskt använder oss löpande av information, är vi i någon mån maktlösa. Vi måste ha koll på det här, säger Per med eftertryck. En parallell som egentligen är på skämt men trots det gravallvarlig, och som ni som befinner er i medberoende på något sätt kan förstå och relatera till, är tolvstegsprogrammet. Väldigt mycket i det handlar om att man inte är ensam i detta. Vi kan utbyta erfarenheter, vi är beroende av varandra och vi är sparringpartners. När man vill landa i ordning och reda, när man vet worst case för sin verksamhet och när man tror att man faktiskt kan hantera jobbet – då är det dags att sätta igång.

Tripnet på väg mot 27001-certifikat

Tripnet har självklart valt att gå för 27001-certifiering och befinner sig just nu i fasen där organisationen ska entusiasmeras och där första offerten är inhämtad.

– Det blir en kul resa, säger Göran. Dessutom gillar vi på Tripnet verkligen när våra kunder kommer till oss och gör olika revisioner. Vi uppskattar det för vi lär oss alltid otroligt mycket då och vi får status på vårt eget dagsläge.

20221129013579

Några heta tips

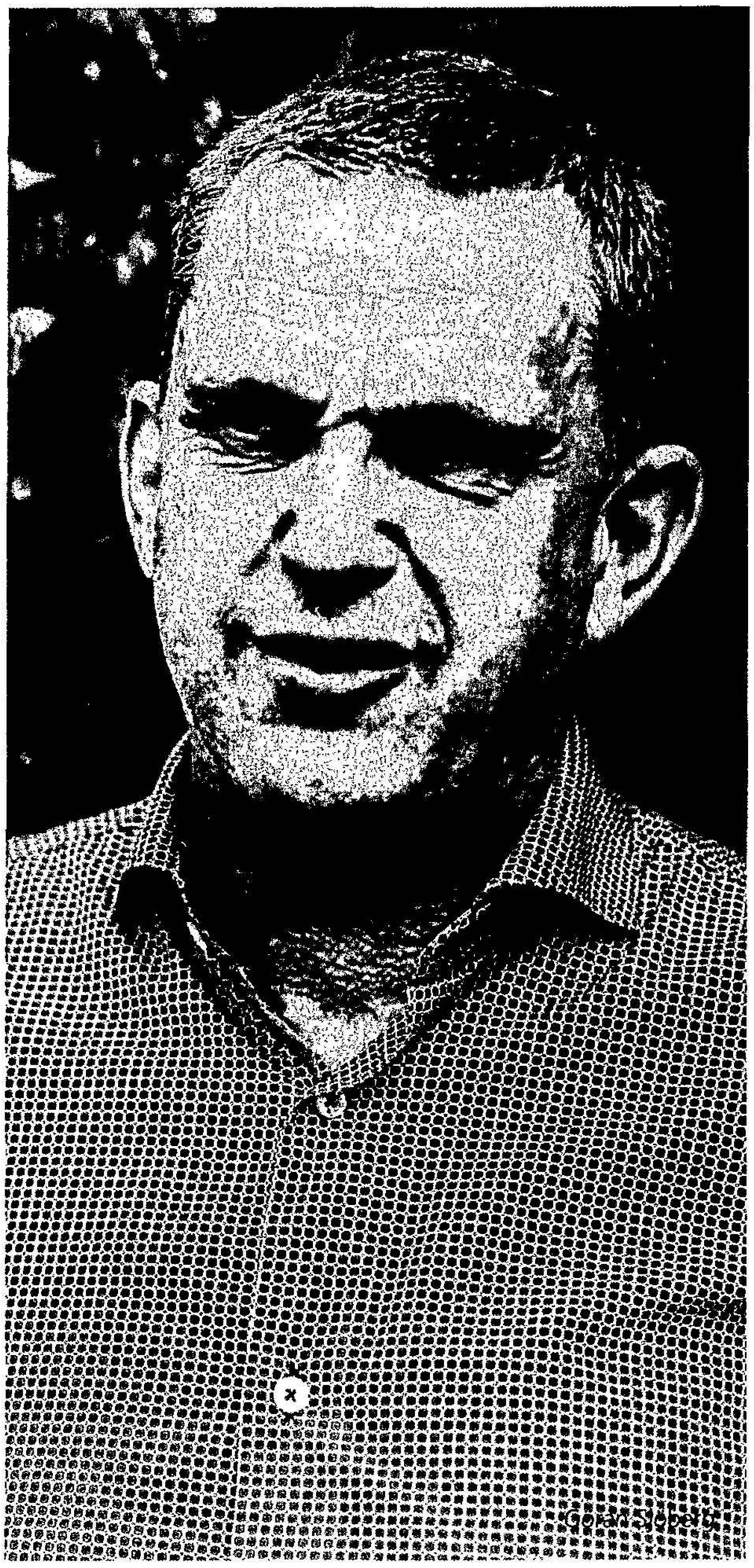
• Bestäm er!
Funderar ni på det, har ni antagligen redan bestämt er.

• Se avvikelser som guld
En avvikelse från revisorn är kunskap att ta fasta på i förbättringsarbetet. Revisorn kan vara verksamhetens bästa vän.

• Entusiasmera hela laget
Tänk utifrån riskbaserad hantering, vilket kan vara omvälvande nytt för vissa. Alla från toppen och neråt måste vara med.

• Besök informationssäkerhet.se
MSB står bakom denna väldigt bra webbsida som ger värdefull kunskap på en tillräckligt bra nivå – en perfekt start.

• Lyssna på Anne-Marie Eklund Löwinders
sommarprat Ratta in Sommar i P1 från 27 juli 2022. Inspirerande och med bra verkshöjd och förklaring till vad detta egentligen handlar om.



20221129001580

Förvaltningsberättelse

Styrelsen och verkställande direktören för Tripnet AB får härmed avge årsredovisning för räkenskapsåret 2021-05-01 – 2022-04-30. Årsredovisningen är upprättad i svenska kronor, SEK.

Verksamheten

Tripnet levererar modern IT-drift för kunder som prioriterar hög säkerhet och tillgänglighet. Vi finns för de som värdesätter personliga relationer, vill bli sedda, söker insiktsfulla råd och uppskattar vårt ansvarstagande.

Vår målgrupp är medvetna kunder med höga krav på bevisad tillgänglighet, konfidentialitet och integritet samt kunder med krav på säkerhetsskyddsklassade system. Vi vet hur man säkerställer rätt säkerhetsnivå för affärs- och samhällskritiska IT-system i såväl, publika molntjänster som Tripnet cloud och datacenter. Publika molntjänster är en naturlig arena för vår kompetens, samtidigt som vår erfarenhet och kontroll över infrastrukturen skapar kundnytta för traditionella enterprisesystem.

Allt fler företag och organisationer upptäcker att bolagets IT-kompetens lämpar sig bäst som strategisk resurs; en kvalificerad beställarorganisation som fokuserar på hur företaget ska behålla och vinna nya kunder genom differentiering, kvalitet och service. Det är klokt. Att använda sin IT-avdelning till att släcka bränder är slöseri med värdefulla resurser. Lösningen är i stället att outsourca med syfte att frigöra tid och resurser för att mer effektivt och fokuserat kunna jobba framåt och utveckla verksamhetsstöd, funktionalitet och verktyg som bidrar till ökad försäljning och bättre lönsamhet.

Väsentliga händelser under räkenskapsåret

Vi har återgått till våra fysiska event och marknadsaktiviteter, såsom Kunskapsfrukostar, julbord och Trailvarvet mm. Våra Kunskapsfrukostar är återigen fysiska, men vi fortsätter streama dessa, vilket innebär att det går att ta del av dem i efterhand.

Under räkenskapsåret har vi fortsatt fokuserat på och stärkt vår roll som rådgivande och proaktiv partner inom samhälls- och affärskritisk IT. Vi har lanserat en ny version av Tripnet Cloud med möjlighet att erbjuda kraftfullare virtuella servers, som möjliggör konsolidering och effektivare licensutnyttjande i mer traditionella enterprisesystem. Vi har under året fortsatt utveckla vår tjänsteportfölj, inte minst inom Informations-, cyber- och IT-säkerhet, där vi ser stor efterfrågan.

Under delar av verksamhetsåret har vi levt med pandemirestriktioner, när dessa slutligen togs bort invaderades Ukraina. Pandemins logistikproblem och komponentbrist har därför fått sällskap av energibrist med höga elpriser, ökad inflation och stigande räntor som följd. Detta gör att några kunder upplevt tuffa tider och att det är svårt att förutsäga framtiden.

Förväntad framtida utveckling

Vårt molnerbjudande och våra säkerhetstjänster fortsätter att vinna mark, såväl i form av erbjudande om drift i

publika moln som vårt eget Tripnet Cloud. Vi ser behovet av rådgivande tjänster inom IT som ständigt ökande.

Vi ser en tillväxt inom säkerhetsområdet, samtidigt som vi ser sjunkande omsättning inom till exempel hårdvarudrift. Vi är inne i en transformationsfas där framtidens erbjudande växer, samtidigt som gamla tjänster fasas ut, kortsiktigt påverkar detta vår omsättning i negativ riktning. På två års sikt ser vi att omsättning och resultat kommer att öka i takt med att vi levererar mer och fler kvalificerade tjänster.

Väsentliga händelser efter räkenskapsårets slut

Vi har lanserat en ny version av vår självprovisioneringstjänst och nya tjänster kring detektering och hantering av illvillig kod och illvilliga operationer. Vi har fortsatt att fokusera på utveckling av vår tjänsteportfölj med fokus på Informations-, cyber- och IT-säkerhet.

Konjunkturläget har försämrats och det råder stor osäkerhet kring såväl räntan som energiförsörjningen. Vår bedömning är att Tripnet inte heller i följdverkningarna av pandemin och fortsättningen av kriget i någon högre grad kommer att påverkas operationellt. De risker vi ser handlar främst om komponentbrist, logistik, energipriser och inflation.

Det finns viss risk för finansiell påverkan för såväl våra kunder som för Tripnet, speciellt om kriget blir långvarigt eller utbrett. Bolaget följer den fortsatta utvecklingen mycket noga och har en förhöjd beredskap för att vid behov kunna agera.

20221129013582

Ägarförhållanden

Bolaget är helägt dotterbolag till Tripnet Holding AB, org. nr. 556742-0582.

Företagets säte

Företaget har sitt säte i Göteborg.

Förslag till vinstdisposition

Styrelsen föreslår att till förfogande stående vinstmedel (kronor):

Balanserad vinst	2 599 923
Årets vinst	146 145
	2 746 068
Disponeras så att	
i ny räkning överföres	2 746 068
	2 746 068

Företagets resultat och ställning i övrigt framgår av efterföljande resultat- och balansräkning samt kassaflödesanalys med noter.

Nyckeltal

Flerårsöversikt (tkr)	2021/22	2020/21	2019/20	2018/19	2017/18
Nettoomsättning	57 915	64 968	59 003	59 203	52 634
Resultat efter finansiella poster	617	6 122	2 185	2 503	2 312
Balansomslutning	28 362	27 710	22 413	23 189	27 105
Soliditet (%)	27	36	30	29	22

För definitioner av nyckeltal, se Redovisnings- och värderingsprinciper.

Förändring av eget kapital	Aktiekapital	Reservfond	Balanserat resultat	Årets resultat	Totalt
Belopp vid årets ingång	127 600	25 000	2 382 812	2 717 110	5 252 522
Disposition enligt beslut av årets årsstämma:					
Utdelning			-2 500 000		-2 500 000
Balanseras i ny räkning			2 717 110	-2 717 110	0
Årets resultat				146 145	146 145
Belopp vid årets utgång	**127 600**	**25 000**	**2 599 922**	**146 145**	**2 898 667**

20221129013S3

Resultaträkning

	Not	2021-05-01 2022-04-30	2020-05-01 2021-04-30
Nettoomsättning		57 914 522	64 968 099
Övriga rörelseintäkter		269 472	239 845
		58 183 994	**65 207 944**
Rörelsens kostnader			
Råvaror och förnödenheter		-13 629 757	-16 009 831
Övriga externa kostnader	1	-18 215 087	-17 873 214
Personalkostnader	2	-23 200 907	-23 163 152
Avskrivningar av materiella och immateriella anläggningstillgångar		-2 012 430	-1 976 849
Övriga rörelsekostnader		-85 108	0
		-57 143 289	**-59 023 046**
Rörelseresultat		**1 040 705**	**6 184 898**
Reslutat från finansiella poster			
Resultat från övriga värdepapper och fordringar som är anläggningstillgångar	3	-341 000	0
Övriga ränteintäkter och liknande resultatposter		0	296
Räntekostnader och liknande resultatposter		-82 351	-62 905
		-423 351	**-62 609**
Resultat efter finansiella poster		**617 354**	**6 122 289**
Bokslutsdispositioner	4	-290 000	-2 600 000
Resultat före skatt		**327 354**	**3 522 289**
Skatt på årets resultat		-181 209	-805 179
Årets resultat		**146 145**	**2 717 110**

20221129015 84

Balansräkning

	Not	2022-04-30	2021-04-30
TILLGÅNGAR			
Anläggningstillgångar			
Immateriella anläggningstillgångar			
Balanserade utgifter för utvecklingsarbeten och liknande arbeten	5	209 312	303 236
Materiella anläggningstillgångar			
Vindkraftverk	6	1 472 000	1 664 000
Inventarier och datacenter	7	4 105 470	4 712 621
		5 577 470	**6 376 621**
Finansiella anläggningstillgångar			
Andra långfristiga värdepappersinnehav	8	2 837 000	0
Andra långfristiga fordringar	9	2 822 000	0
		5 659 000	**0**
Summa anläggningstillgångar		**11 445 782**	**6 679 857**
Omsättningstillgångar			
Varulager m m			
Råvaror och förnödenheter		30 920	0
Kortfristiga fordringar			
Kundfordringar		2 372 430	773 660
Fordringar hos koncernföretag		0	626 580
Aktuella skattefordringar		869 298	82 323
Övriga fordringar		2 303	86 522
Förutbetalda kostnader och upplupna intäkter	10	4 523 769	3 682 946
		7 767 800	**5 252 031**
Kassa och bank	11	9 117 176	15 777 768
Summa omsättningstillgångar		**16 915 896**	**21 029 799**
SUMMA TILLGÅNGAR		**28 361 678**	**27 709 656**

20221129015B5

	Not	2022-04-30	2021-04-30
EGET KAPITAL OCH SKULDER			
Eget kapital	12		
Bundet eget kapital			
Aktiekapital		127 600	127 600
Reservfond		25 000	25 000
		152 600	**152 600**
Fritt eget kapital			
Balanserad vinst eller förlust		2 599 923	2 382 813
Årets resultat		146 145	2 717 110
		2 746 068	**5 099 923**
Summa eget kapital		**2 898 668**	**5 252 523**
Obeskattade reserver	13	**6 160 000**	**5 870 000**
Kortfristiga skulder			
Leverantörsskulder		3 525 299	2 774 510
Övriga skulder		655 045	583 309
Upplupna kostnader och förutbetalda intäkter	14	15 122 666	13 229 314
Summa kortfristiga skulder		**19 303 010**	**16 587 133**
SUMMA EGET KAPITAL OCH SKULDER		**28 361 678**	**27 709 656**

20221129015B6

Kassaflödesanalys

	Not	2021-05-01 2022-04-30	2020-05-01 2021-04-30
Den löpande verksamheten			
Resultat efter finansiella poster		617 354	6 122 289
Justeringar för poster som inte ingår i kassaflödet	15	2 438 538	1 976 849
Betald skatt		-968 183	-466 139
Kassaflöde från den löpande verksamheten före förändring av rörelsekapital		**2 087 709**	**7 632 999**
Kassaflöde från förändring av rörelsekapitalet			
Förändring av varulager och pågående arbete		-30 920	39 680
Förändring av kundfordringar		-1 598 770	1 995 768
Förändring av kortfristiga fordringar		-756 604	708 399
Förändring av leverantörsskulder		750 789	729 563
Förändring av kortfristiga skulder		1 965 088	999 702
Kassaflöde från den löpande verksamheten		**2 417 292**	**12 106 111**
Investeringsverksamheten			
Investeringar i materiella anläggningstillgångar		- 1 204 464	-1 274 198
Investeringar i finansiella anläggningstillgångar		-6 000 000	0
Kassaflöde från investeringsverksamheten		**-7 204 464**	**-1 274 198**
Finansieringsverksamheten			
Utbetald utdelning		-1 873 420	-900 000
Reglerade, lämnade koncernbidrag		0	-800 000
Kassaflöde från finansieringsverksamheten		**-1 873 420**	**-1 700 000**
Årets kassaflöde		**-6 660 592**	**9 131 913**
Likvida medel vid årets början			
Likvida medel vid årets början		15 777 768	6 645 855
Likvida medel vid årets slut		**9 117 176**	**15 777 768**

20221129015587

Redovisnings- och värderingsprinciper

Allmänna upplysningar
Årsredovisningen är upprättad i enlighet med årsredovisningslagen och BFNAR 2012:1 Årsredovisning och koncernredovisning (K3). Företaget är ett mindre företag och har valt att göra detta på frivillig basis.

Redovisningsprinciperna är oförändrade jämfört med föregående år.

Intäktsredovisning
Intäkter har tagits upp till verkligt värde av vad som erhållits eller kommer att erhållas och redovisas i den omfattning det är sannolikt att de ekonomiska fördelarna kommer att tillgodogöras bolaget och intäkterna kan beräknas på ett tillförlitligt sätt.

Förskottsfakturerade intäkter periodiseras till den period som intäkt avser. Förskottsfakturering redovisas under posten upplupna kostnader och förutbetalda intäkter.

Vid försäljning av varor redovisas normalt inkomsten som intäkt när de väsentliga förmåner och risker som är förknippade med ägandet av varan har överförts från företaget till köparen.

Pågående tjänsteuppdrag
För uppdrag på löpande räkning redovisas inkomsten som är hänförlig till ett utfört uppdrag som intäkt i takt med att arbete utförs och material levereras eller förbrukas.

För uppdrag till fast pris redovisas de inkomster och utgifter som är hänförliga till ett utfört uppdrag som intäkt respektive kostnad i förhållande till uppdragets färdigställandegrad på balansdagen (successiv vinstavräkning). Ett uppdrags färdigställandegrad bestäms genom att nedlagda utgifter på balansdagen jämförs med beräknade totala utgifter. I de fall utfallet av ett uppdrag inte kan beräknas på ett tillförlitligt sätt, redovisas intäkter endast i den utsträckning som motsvaras av de uppkomna uppdragsutgifter som sannolikt kommer att ersättas av beställaren. En befarad förlust på ett uppdrag redovisas omgående som kostnad.

Redovisningsprinciper för enskilda balansposter

Immateriella tillgångar
Företaget redovisar internt upparbetade immateriella anläggningstillgångar enligt aktiveringsmodellen. Det innebär att samtliga utgifter som avser framtagandet av en internt upparbetad immateriell anläggningstillgång aktiveras och skrivs av under tillgångens beräknade nyttjandeperiod, under förutsättningarna att kriterierna i BFNAR 2012:1 är uppfyllda.

Anläggningstillgångar
Immateriella och materiella anläggningstillgångar redovisas till anskaffningsvärde minskat med ackumulerade avskrivningar enligt plan och eventuella nedskrivningar.

Avskrivning sker linjärt över den förväntade nyttjandeperioden med hänsyn till väsentligt restvärde. Följande avskrivningsprocent tillämpas:

Immateriella anläggningstillgångar	
Balanserade utgifter för utvecklingsarbeten	20%
Materiella anläggningstillgångar	
Inventarier och datacenter	14-33%
Vindkraftverk	6,67%

Finansiella instrument
Finansiella instrument värderas utifrån anskaffningsvärdet. Instrumentet redovisas i balansräkningen när bolaget blir part i instrumentets avtalsmässiga villkor. Finansiella tillgångar tas bort från balansräkningen när rätten att erhålla kassaflöden från instrumentet har löpt ut eller överförts och bolaget har överfört i stort sett alla risker och förmåner som är förknippade med äganderätten. Finansiella skulder tas bort från balansräkningen när förpliktelserna har reglerats eller på annat sätt upphört.

Andra långfristiga värdepappersinnehav och andra långfristiga fordringar
Placeringar i värdepapper som är anskaffade med avsikt att innehas långsiktigt har redovisats till sina anskaffningsvärden. Varje balansdag görs bedömning om eventuellt nedskrivningsbehov.

Kundfordringar/kortfristiga fordringar
Kundfordringar och kortfristiga fordringar redovisas som omsättningstillgångar till det belopp som förväntas bli inbetalt efter avdrag för individuellt bedömda osäkra fordringar.

Låneskulder och leverantörsskulder
Låneskulder och leverantörsskulder redovisas initialt till anskaffningsvärde efter avdrag för transaktionskostnader. Skiljer sig det redovisade beloppet från det belopp som ska återbetalas vid förfallotidpunkten periodiseras mellanskillnaden som räntekostnad över lånets löptid med hjälp av instrumentets effektivränta. Härigenom överensstämmer vid förfallotidpunkten det redovisade beloppet och det belopp som ska återbetalas.

20221129013B8

Kvittning av finansiell fordran och finansiell skuld
En finansiell tillgång och en finansiell skuld kvittas och redovisas med ett nettobelopp i balansräkningen endast då legal kvittningsrätt föreligger samt då en reglering med ett nettobelopp avses ske eller då en samtida avyttring av tillgången och reglering av skulden avses ske.

Leasingavtal
Företaget redovisar samtliga leasingavtal, såväl finansiella som operationella, som operationella leasingavtal. Operationella leasingavtal redovisas som en kostnad linjärt över leasingperioden.

Varulager
Varulagret har värderats till det lägsta av dess anskaffningsvärde och dess nettoförsäljningsvärde på balansdagen. Med nettoförsäljningsvärde avses varornas beräknade försäljningspris minskat med försäljningskostnader. Den valda värderingsmetoden innebär att inkurans i varulagret har beaktats.

Inkomstskatter
Total skatt utgörs av aktuell skatt och uppskjuten skatt. Skatter redovisas i resultaträkningen, utom då underliggande transaktion redovisas direkt mot eget kapital varvid tillhörande skatteeffekter redovisas i eget kapital.

Företaget har inga temporära skillnader varför inga upplupna skattefordringar eller upplupna skatteskulder redovisas.

Aktuell skatt
Aktuell skatt avser inkomstskatt för innevarande räkenskapsår samt den del av tidigare räkenskapsårs inkomstskatt som ännu inte redovisats. Aktuell skatt beräknas utifrån den skattesats som gäller per balansdagen.

Ersättningar till anställda
Ersättningar till anställda avser alla former av ersättningar som företaget lämnar till de anställda. Kortfristiga ersättningar utgörs av bland annat löner, betald semester, betald frånvaro, bonus och ersättning efter avslutad anställning (pension). Kortfristiga ersättningar redovisas som kostnad och en skuld då det finns en legal eller informell förpliktelse att betala ut en ersättning till följd av en tidigare händelse och en tillförlitlig uppskattning av beloppet kan göras.

Ersättningar till anställda efter avslutad anställning
I företaget finns endast avgiftsbestämda pensionsplaner. Som avgiftsbestämda planer klassificeras planer där fastställda avgifter betalas och det inte finns förpliktelser att betala något ytterligare, utöver dessa avgifter.

Utgifter för avgiftsbestämda planer redovisas som en kostnad under den period de anställda utför de tjänster som ligger till grund för förpliktelsen.

Statliga bidrag
Bidrag från staten redovisas till verkligt värde då det föreligger en rimlig säkerhet att bidraget kommer att erhållas och företaget kommer uppfylla de villkor som är förknippade med bidraget. Statliga bidrag som avser kostnadstäckning periodiseras och intäktsredovisas i resultaträkningen över samma perioder som de kostnader bidragen är avsedda att täcka. Statliga bidrag presenteras som en övrig intäkt i företagets resultaträkning

Koncernbidrag
Erhållna och lämnade koncernbidrag redovisas som bokslutsdispositioner.

Kassaflödesanalys
Kassaflödesanalysen upprättas enligt indirekt metod. Det redovisade kassaflödet omfattar endast transaktioner som medfört in- eller utbetalningar.

Nyckeltalsdefinitioner
Nettoomsättning
Rörelsens huvudintäkter, fakturerade kostnader, sidointäkter samt intäktskorrigeringar.

Resultat efter finansiella poster
Resultat efter finansiella intäkter och kostnader men före bokslutsdispositioner och skatter.

Balansomslutning
Företagets samlade tillgångar.

Soliditet (%)
Justerat eget kapital (eget kapital och obeskattade reserver med avdrag för uppskjuten skatt) i procent av balansomslutning.

Uppskattningar och bedömningar
Företagets ledning bedömer att det inte föreligger väsentliga bedömningar som har betydande effekt på de redovisade beloppen i årsredovisningen.

20221129015B9

Noter

Not 1 Leasingavtal

Årets leasingkostnader avseende leasingavtal, uppgår till 11 566 791 kronor (f å 10 944 339 kronor).

Leasingkostnader utgörs till största delen hyreskostnader för lokaler, utrustning i företagets datacenter samt billeasing.

Not 2 Medelantalet anställda

	2021-05-01 2022-04-30	2020-05-01 2021-04-30
Medelantalet anställda	24	24

Not 3 Resultat från övriga värdepapper och fordringar som är anläggningstillgångar

	2021-05-01 2022-04-30	2020-05-01 2021-04-30
Nedskrivningar	-341 000	0
-341 000	**-0**	

Not 4 Bokslutsdispositioner

	2021-05-01 2022-04-30	2020-05-01 2021-04-30
Avsättning till periodiseringsfond	-290 000	-1 250 000
Återföring från periodiseringsfond	0	500 000
Förändring av överavskrivningar	0	-1 000 000
Koncernbidrag	0	-850 000
-290 000	**-2 600 000**	

Not 5 Balanserade utgifter för utvecklingsarbeten och liknande arbeten

	2022-04-30	2021-04-30
Ingående anskaffningsvärden	1 577 033	1 577 033
Utgående ackumulerade anskaffningsvärden	**1 577 033**	**1 577 033**
Ingående avskrivningar	-1 273 797	-1 179 873
Årets avskrivningar	-93 924	-93 924
Utgående ackumulerade avskrivningar	**-1 367 721**	**-1 273 797**
Utgående redovisat värde	**209 312**	**303 236**

Not 6 Vindkraftverk

	2022-04-30	2021-04-30
Ingående anskaffningsvärden	2 880 000	2 880 000
Utgående ackumulerade anskaffningsvärden	**2 880 000**	**2 880 000**
Ingående avskrivningar	-1 216 000	-1 024 000
Årets avskrivningar	-192 000	-192 000
Utgående ackumulerade avskrivningar	**-1 408 000**	**-1 216 000**
Utgående redovisat värde	**1 472 000**	**1 664 000**

20221129013596

Not 7 Inventarier

	2022-04-30	2021-04-30
Ingående anskaffningsvärden	38 334 124	37 059 926
Inköp	1 204 463	1 274 198
Utrangeringar	-18 115 233	0
Utgående ackumulerade anskaffningsvärden	**21 423 354**	**38 334 124**
Ingående avskrivningar	-33 621 503	-31 930 578
Utrangeringar	18 030 125	0
Årets avskrivningar	-1 726 506	-1 690 925
Utgående ackumulerade avskrivningar	**-17 317 884**	**-33 621 503**
Utgående redovisat värde	**4 105 470**	**4 712 621**

Not 8 Andra långfristiga värdepappersinnehav

	2022-04-30	2021-04-30
Ingående anskaffningsvärden	0	0
Inköp	3 000 000	0
Utgående ackumulerade anskaffningsvärden	**3 000 000**	**0**
Ingående nedskrivningar	0	0
Årets nedskrivningar	-163 000	0
Utgående ackumulerade nedskrivningar	**-163 000**	**0**
Utgående redovisat värde	**2 837 000**	**0**

Not 9 Andra långfristiga fordringar

	2022-04-30	2021-04-30
Ingående anskaffningsvärden	0	0
Tillkommande fordringar	3 000 000	0
Utgående ackumulerade anskaffningsvärden	**3 000 000**	**0**
Ingående nedskrivningar	0	0
Årets nedskrivningar	-178 000	0
Utgående ackumulerade nedskrivningar	**-178 000**	**0**
Utgående redovisat värde	**2 822 000**	**0**

Not 10 Förutbetalda kostnader och upplupna intäkter

	2022-04-30	2021-04-30
Förutbetalda driftskostnader	1 237 144	1 616 504
Förutbetalda lokalkostnader	530 608	531 931
Förutbetalda leasingkostnader	1 313 918	809 392
Övriga förutbetalda kostnader och upplupna intäkter	750 809	725 119
Upplupna intäkter	691 290	0
	4 523 769	**3 682 946**

Not 11 Checkräkningskredit

	2022-04-30	2021-04-30
Beviljat belopp på check-räkningskredit uppgår till	5 000 000	5 000 000
Utnyttjad kredit uppgår till	0	0
Ställda säkerheter		
Företagsinteckning	2 920 000	2 920 000
	2 920 000	**2 920 000**

C2022112901591

Not 12 Antal aktier och kvotvärde

	Antal aktier	Kvotvärde
Aktier	1 276	100
	1 276	

Not 13 Obeskattade reserver

	2022-04-30	2021-04-30
Ackumulerade överavskrivningar	2 600 000	2 600 000
Periodiseringsfond räkenskapsår 2017-04-30	300 000	300 000
Periodiseringsfond räkenskapsår 2018-04-30	400 000	400 000
Periodiseringsfond räkenskapsår 2019-04-30	670 000	670 000
Periodiseringsfond räkenskapsår 2020-04-30	650 000	650 000
Periodiseringsfond räkenskapsår 2021-04-30	1 250 000	1 250 000
Periodiseringsfond räkenskapsår 2022-04-30	290 000	0
	6 160 000	**5 870 000**
Uppskjuten skatt avseende obeskattade reserver	1 303 340	1 264 400

Not 14 Upplupna kostnader och förubetalda intäkter

	2022-04-30	2021-04-30
Förutbetalda intäkter	9 132 420	8 221 074
Upplupna personalkostnader	4 278 967	3 803 518
Övriga upplupna kostnader	1,711,279	1 204 722
	15 122 666	**13 229 314**

Not 15 Justering för poster som inte ingår i kassaflödet

	2022-04-30	2021-04-30
Avskrivningar	2 012 430	1 976 849
Förlust vid utrangeringar av anläggningstillgångar	85 108	0
Nedskrivningar	341 000	0
	2 438 538	**1 976 849**

Not 16 Uppgifter om moderföretaget

Företaget är helägt dotterföretag till Tripnet Holding AB, org. nr. 556742-0582, med säte i Göteborg.

”Tripnet – vilken superbra service! Jag har på kort tid fått stort förtroende för dem.””

20221129013593

Resultat- och balansräkningen kommer att föreläggas på årsstämma för fastställelse.

Göteborg 2022-10-31

Mikael Karlsson
Ordförande

Martin Dohmen
Vice verkställande direktör

Daniel Ryde

Ulf Persson
Verkställande direktör

Min revisionsberättelse har lämnats 2022-10-31.

Håkan Johansson
Auktoriserad revisor

20221129013594

Revisionsberättelse

Till bolagsstämman i Tripnet AB

Org.nr 556507-5362

Rapport om årsredovisningen

Uttalande

Jag har utfört en revision av årsredovisningen för Tripnet AB för räkenskapsåret 2021-05-01 - 2022-04-30. Bolagets årsredovisning ingår i den tryckta versionen av detta dokument på sidorna 32-45.

Enligt min uppfattning har årsredovisningen upprättats i enlighet med årsredovisningslagen och ger en i alla väsentliga avseenden rättvisande bild av Tripnet ABs finansiella ställning per den 2022-04-30 och av dess finansiella resultat och kassaflöde för året enligt årsredovisningslagen. Förvaltningsberättelsen är förenlig med årsredovisningens övriga delar. Jag tillstyrker därför att bolagsstämman fastställer resultaträkningen och balansräkningen.

Grund för uttalanden

Jag har utfört revisionen enligt International Standards on Auditing (ISA) och god revisionssed i Sverige. Mitt ansvar enligt dessa standarder beskrivs närmare i avsnittet Revisorns ansvar. Jag är oberoende i förhållande till Tripnet AB enligt god revisorssed i Sverige och har i övrigt fullgjort mitt yrkesetiska ansvar enligt dessa krav.

Jag anser att de revisionsbevis jag har inhämtat är tillräckliga och ändamålsenliga som grund för mina uttalanden.

Annan information än årsredovisningen

Detta dokument innehåller även annan information än årsredovisningen och återfinns på sidorna 1-31. Det är styrelsen och verkställande direktören som har ansvaret för denna andra information.

Mitt uttalande avseende årsredovisningen omfattar inte denna information och jag gör inget uttalande med bestyrkande avseende denna andra information.

I samband med min revision av årsredovisningen är det mitt ansvar att läsa den information som identifieras ovan och överväga om informationen i väsentlig utsträckning är oförenlig med årsredovisningen. Vid denna genomgång beaktar jag även den kunskap jag i övrigt inhämtat under revisionen samt bedömer om informationen i övrigt verkar innehålla väsentliga felaktigheter.

Om jag, baserat på det arbete som har utförts avseende denna information, drar slutsatsen att den andra informationen innehåller en väsentlig felaktighet, är jag skyldig att rapportera detta. Jag har inget att rapportera i det avseendet.

Styrelsens och verkställande direktörens ansvar

Det är styrelsen och verkställande direktören som har ansvaret för att årsredovisningen upprättas och att den ger en rättvisande bild enligt årsredovisningslagen. Styrelsen och verkställande direktören ansvarar även för den interna kontroll som de bedömer är nödvändig för att upprätta en årsredovisning som inte innehåller några väsentliga felaktigheter, vare sig dessa beror på oegentligheter eller misstag.

Vid upprättandet av årsredovisningen ansvarar styrelsen och verkställande direktören för bedömningen av bolagets förmåga att fortsätta verksamheten. De upplyser, när så är tillämpligt, om förhållanden som kan påverka förmågan att fortsätta verksamheten och att använda antagandet om fortsatt drift. Antagandet om fortsatt drift tillämpas dock inte

20221129015935

om styrelsen och verkställande direktören avser att likvidera bolaget, upphöra med verksamheten eller inte har något realistiskt alternativ till att göra något av detta.

Revisorns ansvar

Mina mål är att uppnå en rimlig grad av säkerhet om huruvida årsredovisningen som helhet inte innehåller några väsentliga felaktigheter, vare sig dessa beror på oegentligheter eller misstag, och att lämna en revisionsberättelse som innehåller mina uttalanden. Rimlig säkerhet är en hög grad av säkerhet, men är ingen garanti för att en revision som utförs enligt ISA och god revisionssed i Sverige alltid kommer att upptäcka en väsentlig felaktighet om en sådan finns. Felaktigheter kan uppstå på grund av oegentligheter eller misstag och anses vara väsentliga om de enskilt eller tillsammans rimligen kan förväntas påverka de ekonomiska beslut som användare fattar med grund i årsredovisningen.

- identifierar och bedömer jag riskerna för väsentliga felaktigheter i årsredovisningen, vare sig dessa beror på oegentligheter eller misstag, utformar och utför granskningsåtgärder bland annat utifrån dessa risker och inhämtar revisionsbevis som är tillräckliga och ändamålsenliga för att utgöra en grund för mina uttalanden. Risken för att inte upptäcka en väsentlig felaktighet till följd av oegentligheter är högre än för en väsentlig felaktighet som beror på misstag, eftersom oegentligheter kan innefatta agerande i maskopi, förfalskning, avsiktliga utelämnanden, felaktig information eller åsidosättande av intern kontroll.

- skaffar jag mig en förståelse av den del av bolagets interna kontroll som har betydelse för min revision för att utforma granskningsåtgärder som är lämpliga med hänsyn till omständigheterna, men inte för att uttala mig om effektiviteten i den interna kontrollen.

- utvärderar jag lämpligheten i de redovisningsprinciper som används och rimligheten i styrelsens och verkställande direktörens uppskattningar i redovisningen och tillhörande upplysningar.

- drar jag en slutsats om lämpligheten i att styrelsen och verkställande direktören använder antagandet om fortsatt drift vid upprättandet av årsredovisningen. Jag drar också en slutsats, med grund i de inhämtade revisionsbevisen, om huruvida det finns någon väsentlig osäkerhetsfaktor som avser sådana händelser eller förhållanden som kan leda till betydande tvivel om bolagets förmåga att fortsätta verksamheten. Om jag drar slutsatsen att det finns en väsentlig osäkerhetsfaktor, måste jag i revisionsberättelsen fästa uppmärksamheten på upplysningarna i årsredovisningen om den väsentliga osäkerhetsfaktorn eller, om sådana upplysningar är otillräckliga, modifiera uttalandet om årsredovisningen. Mina slutsatser baseras på de revisionsbevis som inhämtas fram till datumet för revisionsberättelsen. Dock kan framtida händelser eller förhållanden göra att ett bolag inte längre kan fortsätta verksamheten.

- utvärderar jag den övergripande presentationen, strukturen och innehållet i årsredovisningen, däribland upplysningarna, och om årsredovisningen återger de underliggande transaktionerna och händelserna på ett sätt som ger en rättvisande bild.

Jag måste informera styrelsen om bland annat revisionens planerade omfattning och inriktning samt tidpunkten för den. Jag måste också informera om betydelsefulla iakttagelser under revisionen, däribland de eventuella betydande brister i den interna kontrollen som jag identifierat.

20221129013596

Uttalanden

Rapport om andra krav enligt lagar och andra författningar

Utöver min revision av årsredovisningen har jag även utfört en revision av styrelsens och verkställande direktörens förvaltning för Tripnet AB för räkenskapsåret 2021-05-01 - 2022-04-30 samt av förslaget till dispositioner beträffande bolagets vinst eller förlust.

Jag tillstyrker att bolagsstämman disponerar vinsten enligt förslaget i förvaltningsberättelsen och beviljar styrelsens ledamöter och verkställande direktören ansvarsfrihet för räkenskapsåret.

Grund för uttalanden

Jag har utfört revisionen enligt god revisionssed i Sverige. Mitt ansvar enligt denna beskrivs närmare i avsnittet Revisorns ansvar. Jag är oberoende i förhållande till Tripnet AB enligt god revisorssed i Sverige och har i övrigt fullgjort mitt yrkesetiska ansvar enligt dessa krav.

Jag anser att de revisionsbevis jag har inhämtat är tillräckliga och ändamålsenliga som grund för mina uttalanden.

Styrelsens och verkställande direktörens ansvar

Det är styrelsen som har ansvaret för förslaget till dispositioner beträffande bolagets vinst eller förlust. Vid förslag till utdelning innefattar detta bland annat en bedömning av om utdelningen är försvarlig med hänsyn till de krav som bolagets verksamhetsart, omfattning och risker ställer på storleken av bolagets egna kapital, konsolideringsbehov, likviditet och ställning i övrigt.

Styrelsen ansvarar för bolagets organisation och förvaltningen av bolagets angelägenheter. Detta innefattar bland annat att fortlöpande bedöma bolagets ekonomiska situation och att tillse att bolagets organisation är utformad så att bokföringen, medelsförvaltningen och bolagets ekonomiska angelägenheter i övrigt kontrolleras på ett betryggande sätt. Verkställande direktören ska sköta den löpande förvaltningen enligt styrelsens riktlinjer och anvisningar och bland annat vidta de åtgärder som är nödvändiga för att bolagets bokföring ska fullgöras i överensstämmelse med lag och för att medelsförvaltningen ska skötas på ett betryggande sätt.

Revisorns ansvar

Mitt mål beträffande revisionen av förvaltningen, och därmed mitt uttalande om ansvarsfrihet, är att inhämta revisionsbevis för att med en rimlig grad av säkerhet kunna bedöma om någon styrelseledamot eller verkställande direktören i något väsentligt avseende:

- företagit någon åtgärd eller gjort sig skyldig till någon försummelse som kan föranleda ersättningsskyldighet mot bolaget, eller

- på något annat sätt handlat i strid med aktiebolagslagen, årsredovisningslagen eller bolagsordningen.

Mitt mål beträffande revisionen av förslaget till dispositioner av bolagets vinst eller förlust, och därmed mitt uttalande om detta, är att med rimlig grad av säkerhet bedöma om förslaget är förenligt med aktiebolagslagen.

20221129013597

Rimlig säkerhet är en hög grad av säkerhet, men ingen garanti för att en revision som utförs enligt god revisionssed i Sverige alltid kommer att upptäcka åtgärder eller försummelser som kan föranleda ersättningsskyldighet mot bolaget, eller att ett förslag till dispositioner av bolagets vinst eller förlust inte är förenligt med aktiebolagslagen.

Som en del av en revision enligt god revisionssed i Sverige använder jag professionellt omdöme och har en professionellt skeptisk inställning under hela revisionen. Granskningen av förvaltningen och förslaget till dispositioner av bolagets vinst eller förlust grundar sig främst på revisionen av räkenskaperna. Vilka tillkommande granskningsåtgärder som utförs baseras på min professionella bedömning med utgångspunkt i risk och väsentlighet. Det innebär att jag fokuserar granskningen på sådana åtgärder, områden och förhållanden som är väsentliga för verksamheten och där avsteg och överträdelser skulle ha särskild betydelse för bolagets situation. Jag går igenom och prövar fattade beslut, beslutsunderlag, vidtagna åtgärder och andra förhållanden som är relevanta för mitt uttalande om ansvarsfrihet. Som underlag för mitt uttalande om styrelsens förslag till dispositioner beträffande bolagets vinst eller förlust har jag granskat om förslaget är förenligt med aktiebolagslagen.

Partille 2022-10-31

Håkan Johansson
Auktoriserad revisor

20221129061598

TRIPNET

Tripnet AB · Åvägen 40 · 412 51 Göteborg · Tel 031-725 25 00 · info@tripnet.se · tripnet.se