kista
SCIENCE CITY

SÄKER DIGITALISERING INOM MEDTECH

Analys av branschens risker

I SAMARBETE MED

tillväxtverket

MED STÖD AV REGION STOCKHOLM

EUROPEISKA UNIONEN
Europeiska regionala utvecklingsfonden

1. FÖRORD

I ett digitaliserat samhälle är cybersäkerhet en avgörande fråga för företag av alla storlekar. I Sverige är dock kunskapen om cybersäkerhet fortfarande låg, särskilt bland små och medelstora företag (SMF). Medicinteknikbranschen är särskilt utsatt där allt fler produkter kopplar upp sig i takt med att verksamheter digitaliseras.

Händelser i omvärlden bidrar till en allt större hotbild och behovet av strukturerad och strategisk cybersäkerhet har aldrig varit större. Samtidigt saknar många SMF fortfarande förståelse, kunnande och resurser för att kunna säkra sina verksamheter. Detta är en oroande utveckling, eftersom cyberattacker mot SMF'er kan få betydande konsekvenser för både företaget självt för kunder och leverantörer.

Kista Science City och Södertälje Science Park har, med stöd av Region Stockholm, och den Europeiska regional utvecklingsfonden (Eruf), under 2022 och 2023 genomfört ett projekt inom cybersäkerhetsområdet med målgrupp SMF, med syfte att att sprida kunskap och etablera ett strategiskt affärsutvecklingsprogram inom cybersäkerhet.

För att öka förståelsen för målgruppen och deras förhållningssätt till cybersäkerhet gjordes en studie på små och medelstora företag inom medicinteknikbranschen. Studien visade att företag inom medicinteknikbranschen är särskilt utsatta för cyberattacker.

Studien påvisar att företagen generellt har en låg riskmedvetenhet och att de saknar en strukturerad säkerhetsstrategi. Vidare visar studien på att medtech bolag är särskilt utsatta för cyberattacker då de ofta hanterar känslig patientinformation.

Karin Bengtsson,

VD Kista Science City

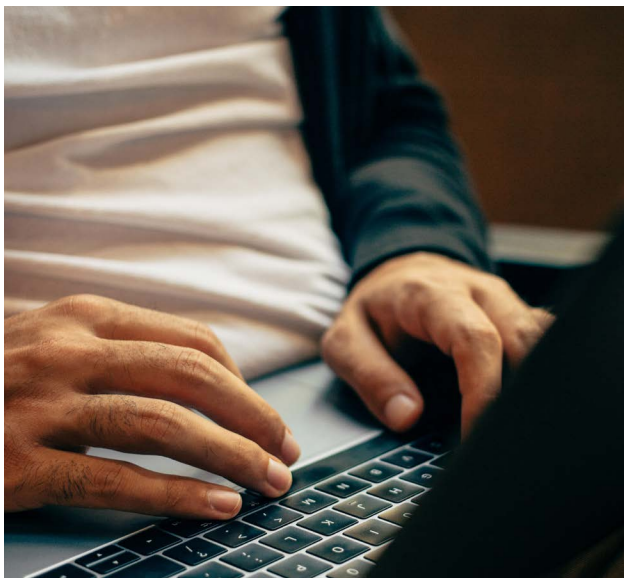
2. SAMMANFATTNING

På senare år har hälso- och sjukvården utsatts för en ökande andel intrång och cyberattacker. Medicinteknikbranschen erbjuder sjukvården många viktiga tjänster, där uppkopplade system gör användningen enklare och förenklar även integreringen av olika medicinska apparater och system. Samtidigt medför det risker om systemet blir tillgängligt för obehöriga aktörer.

Flera nya regelverk för att öka säkerheten för medicintekniska produkter är på gång att införas inom EU. Ett exempel är en utökad version av nätverks- och informationssäkerhetsdirektivet, NIS, kallat NIS2, som ska omfatta medicintekniska produkter och medicintekniska produkter för in vitro-diagnostik. Senast i oktober 2024 ska det vara införlivat i medlemsländernas lagstiftning.

För att få en bild av hur medicinteknikföretagen arbetar med säkerhet gjordes en kvalitativ studie med frågeställningen: Hur arbetar små och medelstora medtechföretag för att motverka risker och hot inom cybersäkerhet? Totalt gjordes 15 intervjuer, varav 13 med medicinteknikföretag, en med Läkemedelsverket samt en med personer inom en region. Intervjuerna analyserades med hjälp av tematisk analys, vilket resulterade i sju teman.

Företagen bedömde generellt att risken för intrång var låg, medan digitala tjänster eller anslutna produkter som brukas av slutanvändare uppfattades som mer utsatta. Lagkrav och krav från vården, samt från eventuella investerare, motiverade de intervjuade att arbeta med informationssäkerhet. Enligt studien saknade dock en väsentlig del av företagen en utarbetad plan för ett eventuellt intrång eller incident. Flera företag var kritiska mot de nya regelverken, eftersom arbetet som krävs för att uppnå kraven ansågs vara för omfattande för att mindre verksamheter skulle klara av det. Däremot var Läkemedelsverket och regionen av åsikten att kraven var både rimliga och nödvändiga. Resultaten avslöjar ett behov av mer samsyn och dialog mellan olika aktörer samt ett behov av regulatoriskt stöd till små och medelstora företag.



I det sista kapitlet kommenterar informationssäkerhetsexpert Marianne Rilde Björkman studiens resultat, samt berättar om ett affärsutvecklingsprogram i strukturerat informations- och cybersäkerhetsarbete, riktad till medicinteknikföretag, som genomförts vid Kista Science City under våren 2023. Hon lyfter vikten av att medvetandegöra alla medarbetare om riskerna då allt inte handlar om attacker, utan också om egna handhavandefel och misstag.

3. DEFINITIONER OCH ORDFÖRKLARING

Definition av centrala begrepp

Anmälda organ (Notified Bodies på engelska). Är oberoende företag som, i vissa fall, på uppdrag av en tillverkare kontrollerar att produkter uppfyller ställda krav på till exempel säkerhet innan de släpps ut på marknaden. Detta sker genom provning, kontroll och certifiering.

CE-märkning. En produktsäkerhetsmärkning som lagstadgats inom EU och där CE står för Conformité Européenne.

Cybersäkerhet. Skyddet mot obehörig eller kriminell användning av elektroniska data och praxis för att säkerställa integritet och tillgänglighet av information.

Digitalisering. Användandet av digital teknik för att förbättra eller förändra sin affär. Digitalteknik. Grundläggande teknik bakom elektroniska apparater och system.

DDoS-attack, En DDoS-attack (Distributed Denial-of-Service attack) är en teknik som används genom att ett stort antal datorer deltar i attacken. Detta gör att det inte effektivt kan avvärjas genom att begränsa trafiken från enskilda IP-adresser. En DDoS-attack kan riktas mot ett nätverk, en webbplats, ett datorsystem eller en webbtjänst

Informationssäkerhet. Att bevara informationens konfidentialitet, riktighet och tillgänglighet. Konfidentialitet betyder att informationen är tillgänglig endast för de personer som har behörighet ta del av den. Riktighet betyder att innehållet i informationen ska vara korrekt och inte kunna förändras av obehöriga. Tillgänglighet betyder att informationen ska vara nåbar när den behövs.

IT-säkerhet. IT-säkerhet är inriktad på att skydda digitala system, data, nätverk, och datorer mot interna och externa hot såsom cyberattacker.

Medicinteknik. Enligt Läkemedelsverket innefattar begreppet medicintekniska produkter som används inom alla delar av hälso- och sjukvården. Exempel är kompresser, kontaktlinsprodukter, sprutor, kanyler, medicinska programvaror och appar, infusionsaggregat och pumpar för läkemedelstillförsel. Produkterna används också av enskilda för egenvård och som hjälpmedel i vardagen.

Nätfiske. Då en individ genom e-post eller sms vilseleds att exempelvis klicka på en länk, köra ett program eller mata in inloggningsuppgifter i syfte att komma åt personliga uppgifter.

Ransomware. Skadlig programvara som låser exempelvis datorer och mobiltelefoner, eller som krypterar filer.

FÖRKORTNINGAR:

CIA – Confidentiality, Integrity, Availability

ENISA – Den europeiska myndigheten för cybersäkerhet

EU – Europeiska unionen

IP – Immateriell tillgång, från engelskans ”intellectual property”

IVDD – In Vitro Diagnostic Medical Devices Directive

IVDR – In Vitro Diagnostic Medical Devices Regulation

KRT – Konfidentialitet, Riktighet, Tillgänglighet

MDCG – Medical Device Coordination Group

MDD – Medical Device Directive

MDR – Medical Device Regulation

MSB – Myndigheten för samhällsskydd och beredskap

NCSI – National Cyber Security Index

NIS – Nätverks- och informationssäkerhetsdirektivet

NIS2 – Uppdaterad NIS-direktiv som innebär utökad version av NIS

SHK – Stockholms handelskammare

SMF – Små och medelstora företag

VPN – Virtual Private Network, för att säkra anslutning till wifi

4. HUR SER SÄKERHETSLÄGET UT I DAG?

Ett populärt exempel på problemet med att uppkopplad medicinteknik kan utsättas för en fientlig attack kommer från populärkulturen. I TV-serien Homeland dödas vicepresidenten i andra säsongens tionde avsnitt av en terrorist som hackar sig in i hans pacemaker och får hans puls att rusa. Scenariot har bäring på verkligheten då både forskare och andra visat att detta går att göra. Och redan fem år innan seriens tragiska dödsfall inaktiverar den dåvarande vicepresidenten Dick Caneys kardiolog för säkerhets skull hans pacemakers trådlösa funktioner. Anslutningen eller ”fjärrövervakningen” som används av den senaste generationen pacemakerenheter gör dem till en idealisk kandidat för att hackas.

Fyra av fem intrång sker inom vården

Hälso- och sjukvården i stort är hårt drabbad av cyberattacker. Enligt Safety Detectives rapport Healthcare Cybersecurity: The Biggest Stats and Trends in 2023 utgör företag i hälso- och sjukvårdsbranschen de mest drabbade vad gäller cyberattacker. Under 2020 stod dataintrång inom hälso- och sjukvårdssektorn för 79 procent av alla intrång. En sammanställning av de tio största visar att de drabbade 160 miljoner patienter. Det största av dem, som gällde ett amerikanskt försäkringsbolag, handlade om 80 miljoner människors personuppgifter.

Patientjournaler innehåller personliga data som kan utnyttjas av tredje part. Till skillnad från ett kreditkort som kan spärras är dessa uppgifter, som personnummer, försäkringsinformation eller diagnoser, icke-förändringsbara och kan därför exponera personen för cyberbrott över lång tid. Ytterligare en aspekt gäller om genetiska data faller i orätta händer – det drabbar inte bara den personen, utan även släktingar.

Krävs på lösensumma för att återfå data

Ransomware är skadlig programvara som låser exempelvis datorer och mobiltelefoner, eller som krypterar filer. För att få tillgång till sina data krävs företaget på en lösensumma, ofta i något slags kryptovaluta som inte är spårbar. Att betala en lösensumma är dock ingen garanti för att återfå sin information.

Här är ett exempel WannaCry som 2017 drabbade den brittiska sjukvården och kostade skattebetalarna 92 miljoner pund efter att 19 000 vårdbesök maliciöst bokades av.

Men även så kallade distributed denial of services-attacker drabbar hälso- och sjukvårdssektorn. Även medicinteknisk utrustning går att skada för att få ägaren att betala en lösensumma. Via dessa uppkopplade apparater går det också att få access till servrar som i sin tur kan vittjas på persondata.

Efter att drabbade tydligt har uppmanats att inte betala lösensumma syns en minskning.

Tre av fyra svenska företagare utsatta

Så hur ser det då ut i Sverige när det gäller risken för cyberattacker? Enligt rapporten Är det IT-säkert? från Företagarna, har 76 procent av Sveriges företagare blivit utsatta för IT-relaterad brottslighet vid minst ett tillfälle under det senaste året.

Vanligast är nätfiske, där 55 procent av de tillfrågade svarade att de hade mottagit e-post från en avsändare som utgav sig för att vara någon annan, i syfte att få tillgång till personliga uppgifter (se ruta).

Många sätt att komma åt data

Nedan beskrivs några vanliga metoder. Förutsättningen för att de ska kunna användas är att det finns en eller flera sårbarheter, som brister i autentiseringsmekanismer eller behörighetshantering, ouppdaterade it-system, övertro på antivirus-produkter eller aktiva konton för medarbetare som inte längre arbetar kvar.

• Lösenordsattacker där man forcerar fram lösenord, för att få tillgång till nätverket.

• Via e-post sker nätfiske, som riktas brett i syfte att få mottagaren att klicka på en länk eller liknande och spearphising, som inkluderar personliga detaljer som ska få mottagaren att agera.

• Vattenhålsangrepp där man till skillnad mot nätfiske placerar skadlig kod på en hemsida och sedan väntar på att besökare ska komma dit.

• Webbattacker som gör att information i bakomliggande databaser kan läsas eller förändras.

• Angrepp mot mjukvaruleverantör, så kallade supply chain-angrepp. Ett exempel var när Coops underleverantör för betalsystem slogs ut och låste Coops kassasystem så att butiker fick hålla stängt.

• Angrepp mot mobila enheter. Ett exempel var säkerhetsbrister i Googles och Samsungs kameraapplikationer i mobiltelefoner som upptäcktes 2019. Dessa gjorde att utomstående kunde få full kontroll över mobiltelefonens kamera, och på distans ta foton, spela in video, lyssna på samtal och lokalisera mobiltelefonens position.

• Fysisk åtkomst, där man via USB-sticka eller med hjälp av en insider för in skadlig kod i ett nätverk.

KÄLLA: Nationellt cybersäkerhetscenters rapport Cybersäkerhet i Sverige 2022. Del 1: Hot, metoder och beroenden.

Finns brister inom cybersäkerhet

National Cyber Security Index, NCSI, rankar Sverige som nummer 26 på en global skala, med ett index på 84.42 av 100. Enligt Myndigheten för samhällsskydd och beredskap har Sverige kunnat stiga här bland annat genom ökat antal utbildningar inom cybersäkerhet och att regeringen genomfört en nationell strategi för samhällets informations- och cybersäkerhet.

Riksrevisionen har dock granskat regeringens arbete för att stärka Sveriges informations- och cybersäkerhet och funnit att det inte är effektivt, vilket man beskriver i Regeringens styrning av samhällets informations- och cybersäkerhet – både brådskande och viktig (RiR 2023:8) från april i år. Riksrevisionen skriver att det dels beror på brister i den nationella informations- och cybersäkerhetsstrategin, dels på att regeringarnas styrning under åren varit svag och splittrad.

Cyberbrott orsakar stora problem

Cyberbrott skapar stora problem, och även om kostnaderna är höga kan det faktum att verksamheten störs vara väl så allvarligt. Enligt Telias Digitala Index 2022 var fler än 200 000 företag i Sverige medvetna om att de hade drabbats av cyberbrott under 2022. Av de drabbade företagen uppger knappt hälften, 44 procent, att de är helt återställda ett år efter attacken. Det kan handla om att kunddata försvunnit, att företagets betalningslösningar inte fungerar eller att hemsidor ligger nere.

Stockholms Handelskammare, SHK, lyfter i rapporten Cyberbrott mot svenska företag – hur bygger vi en säkrare framtid? de höga kostnader som är förenade med att drabbas av cyberbrott. Kostnaden som dessa orsakade svenska företag under 2021 beräknas till 30 miljarder kronor, en fördubbling jämfört med 2019.

Globalt motsvarar cyberangrepp den tredje största ekonomin, efter Kina och USA, enligt Telias Digitala Index 2022.

I takt med att allt fler är uppkopplade, ökar också exponeringsytan som kan användas för intrång. I dag använder fem miljarder människor internet. Tillsammans äger vi omkring 30 miljarder enheter – mobiltelefoner, larmsystem, skrivare, pacemakers, aktivitetsarmband med mera som är uppkopplade mot internet.

11 MILJONER NYA ENHETER KOPPLAS UPP VARJE DYGN GLOBALT

I dag uppskattas 127 nya enheter anslutas till internet per sekund, dygnet runt och året om – vilket också kan uttryckas som 11 miljoner nya enheter per dygn.

KÄLLA: SHKs rapport Cyberbrott mot svenska företag – hur bygger vi en säkrare framtid?

Få cyberbrott polisanmäls

Men även om många företag drabbas av cyberbrott är viljan att polisanmäla låg. I Företagarnas rapport Är det IT-säkert? anger man siffran 13 procent. Anledningen är att man inte tror att polisen kommer att kunna klara upp brottet, vilket också verkar stämma i många fall – 69 procent av de anmälda cyberbrotten lades ner. Totalt ledde bara en procent av de anmälda brotten till åtal.

I SHKs rapport anges ytterligare en anledning, nämligen negativ uppmärksamhet i media. En källa uttrycker det här som att ”många företagsledare anser att det är lite fult att ha blivit hackad, ungefär som att ha fått en könssjukdom”.

Medicinteknikföretag riskerar konkurs vid attack

Den nya studie som beskrivs i kapitel 6 och 7 visar att små och medelstora företag i medicinteknikbranschen inte är så motiverade att arbeta med sin cybersäkerhet. Dels för att man inte uppfattar att riskerna är så stora, dels då man anser att de åtgärder som krävs tar för mycket resurser.

En motiverande faktor kan vara att ta fram ett scenario som gestaltar hur kostsamt ett angrepp skulle kunna bli. Ett sådant scenario för just ett medicinskt tekniskt företag beskrevs förra året (se ruta). Där konstaterar skribenterna att de summor som det fiktiva företaget skulle behöva betala är astronomiska och sannolikt leder till konkurs.

Ett möjligt scenario

Exemplet gäller i korta drag ett fiktivt USA-baserat företag vars produkt är det inplanterbara chipet LessDepressed. Det monitorerar signalämnen i hjärnan och initierar behandling genom att släppa ut lämplig substans. Det rapporterar tillbaka till företaget som kan använda data för maskininlärning och kopplas via BlueTooth till en mobilapp så att patienter och anhöriga kan följa monitoreringen i realtid.

När cyberattacken sker bär 10 000 personer chipet. För att återfå kontrollen måste företaget betala 15 miljoner dollar i bitcoin inom 48 timmar. Företagets lyckas få 5000 patienter att avinstallera appen som kopplas till chipet. Men efter 48 timmar slår förövaren ut resten av chipen och gör dem obrukbara.

Alla dessa 5000 obrukbara chip måste opereras ut på företagets bekostnad. Företaget hyrde också in kostsamma konsulter för att – förgäves visade det sig – försöka lösa det uppkomna problemet. Dessutom blir det rättsliga efterspel med stämningar och skadestånd, plus en medieskandal som utarmar förtroendet för företaget och produkten.

USA och Sverige är inte direkt jämförbara, men skribenterna konstaterar att de summor som företaget behöver betala är astronomiska och att konkurs är sannolikt.

KÄLLA: Medtech Cyber-Incidents: A Costlier Problem Than You Think, Med Device Online, 17 augusti 2022.

5. SÅ REGLERAS MEDICINTEKNISKA PRODUKTERS SÄKERHET

Medicintekniska produkter är en central del av hälso- och sjukvården och att systemen fungerar som de ska kan vara livsavgörande. De omfattas därför av regelverk, certifieringssystem och standarder. Här beskrivs de övergripande regelverk och förordningar som gäller inom EU. Dessa utökas nu och skärps, något som i sin tur påverkar de företag som tillverkar medicintekniska produkter och system.

Inom EU finns sedan 1993 ett direktiv kallat MDD, från engelskans Medical Device Directive. För implanterbara apparater finns direktiv sedan 1990 och för in vitro-apparater sedan 1998, förkortat IVDD, från engelskans In Vitro Diagnostic Medical Devices Directive.

För att förenkla harmoniseringen och uppdatera säkerhetskraven har nya regelverk tagits fram av den europeiska kommissionen som ska ersätta dessa båda direktiv, mer om dessa nedan.

En annan viktig del av marknadskontrollen för medicintekniska produkter är CE-märkning, en produktsäkerhetsmärkning som lagstadgats inom EU och där CE står för Conformité Européenne. Med CE-märkningen intygar en tillverkare eller importör att produkten uppfyller kraven vilket innebär att produkten kan säljas fritt inom EUs medlemsländer. Tillverkaren avgör om man själv har kompetens att bedöma sin produkt, eller om ett oberoende certifieringsorgan behöver användas, på engelska a notified body, som på svenska kallas anmält organ. Medicintekniska produkter delas in i fyra riskklasser (se ruta).

Fyra riskklasser för medicintekniska produkter

Medicintekniska produkter delas in i fyra klasser beroende på hur allvarlig risk som produkten kan medföra för patienten. Den högsta identifierade riskklassningen utgör produktens riskklass. Faktorer som styr klassificeringen är exempelvis hur länge produkten förväntas vara i bruk, eller om den används invärtes eller utvärtes.

• Klass I är den lägsta riskklassningen. Till skillnad från de högre klasserna krävs inte regelbunden uppföljning av ett anmält organ. Under denna riskklass faller exempelvis bandage och rullstolar.

• Klass IIa omfattar produkter med måttlig risk. Alla medicintekniska produkter som kräver energitillförsel, så kallade aktiva apparater, faller i denna riskklass eller högre. Även mjukvara räknas som aktiv apparat.

• Klass IIb ges vid måttlig/hög risk. Här ingår exempelvis diagnostiska verktyg som mäter livsviktiga funktioner som syresättning eller puls och ger stöd för diagnoser, samt apparater som avger strålning.

• Klass III är den högsta riskklassningen. Här ingår implanterbara apparater och produkter som används i mer än sex månader, samt apparater som doserar medicin eller stödjer livsviktiga funktioner.

Nya regelverk är på gång

Som nämndes ovan kommer två nya förordningar från EU-kommissionen som berör olika slags medicinska apparater. En trädde i kraft den 26 maj 2021 och förkortas MDR, från engelskans Medical Device Regulation. Dess kriterier ska följas efter att övergångsperioden går ut 26 maj 2024. En förlängd deadline gör dock att produkter kan fortsätta under tidigare direktiv fram till 26 maj 2026, 31 december 2027 eller 31 december 2028, beroende på den medicintekniska produktens riskklass.

En liknande förordning, förkortad IVDR från engelskans In Vitro Diagnostic Regulation, berör medicinska in vitro-apparater, som analyserar blod och vävnad. Denna förordning trädde i kraft den 26 maj 2022 och ersatte tidigare direktiv. Övergångsperioden för dessa apparater gäller till 26 maj 2025. En förlängd deadline, enligt ovan, gäller även för denna förordning och innebär att övergångsperioden kan förlängas till maj 2026 eller maj 2027.

De krav som ges i MDR och IVDR är förhållandevis öppna för tolkning. Därför har ett vägledande dokument tagits fram av Medical Device Coordination Group, MDCG. Här samlas konkreta åtgärder och andra relevanta regelverk för informationssäkerhetskrav.

Olika standarder ger stöd

Dagens regelverk i EU bygger på utpekade så kallade harmoniserade standarder som produkterna ska följa. Standarder kan enkelt beskrivas som ”strukturerat sunt förnuft” och i Sverige finns ett stort antal standarder som beskriver medicintekniska produkter och som bygger på europeiska och internationella standarder (se ruta).

Den så kallade ISO 27000-serien baseras på att skydda information och eftersom informationen i dag ofta finns digitaliserad omfattar den även cybersäkerhet. I princip alla organisationer har även information som innehåller personuppgifter och därför har serien utökats till att även omfatta dataskydd.

I standarden ISO 27000-serien definieras informationssäkerhet som bevarandet av konfidentialitet, riktighet och tillgänglighet, KRT.

Standarder för medicintekniska produkter

För medicintekniska företag finns olika standarder som stöd och utgångspunkt för att möta kraven som gällande och kommande förordningar från EU ställer.

- ISO 13485 beskriver lämpliga åtgärder vid implementeringen av ett kvalitetshanteringssystem för medicinska apparater.
- ISO 14971 gäller riskhantering för medicinska apparater med ett ramverk för att utvärdera och identifiera eventuella risker.
- IEC 62304 beskriver processer för hanteringen av mjukvara i medicinska apparater samt ett antal lämpliga processer för underhåll under apparatens livscykel.
- IEC 80001 serien berör riskhantering för it-nätverk som ansluter medicinska apparater och specificerar ett antal krav samt ansvarsfördelning och föreslår ett antal lämpliga säkerhetsmönster.

Bristande informationssäkerhet kan ge höga böter

Inom EU gäller även NIS, nätverks- och informationssäkerhetsdirektivet, som trädde i kraft i svensk lag i juli 2018. Det omfattar sju samhällsviktiga verksamheter, bland annat hälso- och sjukvård. Direktivet ställer krav på att berörda verksamheter ska arbeta systematiskt och riskbaserat, samt rapportera incidenter till respektive sektorsansvariga myndigheter. Senast i oktober 2024 ska det nya och mer omfattande NIS2-direktivet vara införlivat i EU-ländernas nationella lagstiftning. Nya sektorer som omfattas av NIS2 är bland annat tillverkning av medicintekniska produkter och medicintekniska produkter för in vitro-diagnostik. Kraven gäller framför allt tydlig riskhantering, incidentupptäckt och -hantering, samt säkerhet i applikationer och infrastruktur. De företag som inte uppfyller NIS2-direktivet riskerar böter på upp till tio miljoner euro, eller två procent av företagets globala omsättning.

Att flera nya och mer omfattande regelverk är på gång påverkar hur svenska medicintekniska företag behöver arbeta med sin cybersäkerhet framöver.

6. HUR SER SMÅ OCH MEDELSTORA MEDICINTEKNIKFÖRETAG PÅ SÄKERHETSHOTEN?

Det förra kapitlet beskriver de nya och mer omfattande regelverk som rör företag som tillverkar medicintekniska produkter. Mot denna bakgrund är det intressant att få en bild av hur företagen i dagsläget ser på riskerna med säkerhetsintrång. Här riktades blicken specifikt mot små och medelstora företag, SMF. Dessa definieras som företag med färre än 250 anställda, med mindre än 50 miljoner euro i årsomsättning.

Angus Bergman, vid Institutionen för data- och systemvetenskap vid Stockholms universitet, undersökte detta i sitt examensarbete *Säker digitalisering inom medtech*: Hur arbetar medtechföretag för att motverka risker och hot inom cybersäkerhet? som utfördes i samarbete med Kista Science City AB. Den fråga som studien skulle besvara var ”Hur förhåller sig medtechbranschen till cybersäkerhet?”.

Under våren 2023 gjorde han en kvalitativ undersökning baserad på 15 intervjuer (se ruta). Intervjuerna transkriberades och med hjälp av tematisk analys kunde svaren grupperas i sju olika teman, se nedan. I följande text har intervjucitaten kortats

Så utfördes studien

• Företagen var små och medelstora företag inom medtech/digitala vårdstjänster.

• Sammanlagt gjordes 15 intervjuer, varav 13 med representanter från lika många företag i olika stadier, med mellan 2 och 160 anställda.

• Dessutom intervjuades en representant för tillsynsmyndigheten Läkemedelsverket, samt två representanter för en region, som är vårdgivare och kund.

• De intervjuade arbetade antingen inom informationssäkerhet internt på företaget, externt hos kunder, eller var beslutsfattare. För att de skulle kunna prata fritt är svaren anonymiserade och den intervjuade kunde välja att inte svara på känsliga frågor.

• Intervjuerna tog mellan 24 och 63 minuter. Svaren transkriberades och utifrån det materialet gjordes en tematisk analys.

• De sju teman som identifierades var: risker och upplevd utsatthet, följder av intrång, hinder för att arbeta med säkerhet, åtgärder mot cyberhot, motivation att arbeta med frågan, kravställning samt digitalisering inom vården generellt.

• Läs hela det slutliga examensarbetet här: www.diva-portal.se

TEMA 1: RISKER OCH UPPLEVD UTSATTHET

Det första temat var upplevda risker. Här uppfattade de intervjuade företagen att risken för en fientlig attack generellt sett var låg, främst på grund av att företaget var litet och inte så synligt.

”Vår app har funnits i tio år, så vi har hållit på länge. Och länge var säkerhetsstrategin att ”vi är så små och vi syns inte”, ”vi har inte så viktig information”.”

De förhöjda risker man ändå såg gällde uppkopplad teknik eller tjänster som används direkt av konsumenter eller i vården. Ett annat problem var slutanvändare som ”hackar utrustning” – exempelvis föräldrar som manipulerar sina barns insulinpumpar. Även externa konsulter i olika form pekades ut som möjlig risk.

”Många tillhör ju inte bolaget, de jobbar som konsulter och gud vet vad de har med sig, det är inte våra datorer.”

Specifika säkerhetsrisker som de intervjuade nämnde var ransomware och nätfiske. Vad gällde just nätfiske upplevde de med färre anställda lägre risk eftersom medarbetarna arbetar med tekniska frågor.

20%

av små och medelstora företag drabbades av intrång 2022

Att små och medelstora företag skulle vara förskonade från attacker stämmer inte. Hela 20 procent av dessa drabbades av intrång 2022, men mörkertalet är stort.

KÄLLA: Telias Digitala Index 2022.

TEMA 2: FÖLJDER AV INTRÅNG

Det andra temat handlar om följderna av ett intrång. Något som man pekade på var risken för förändringar i sådana forskningsdata som krävs för att få tillgång till marknaden, exempelvis om det i en dubbelblind, placebokontrollerad studie skulle läcka ut vilken patient som fått verksam behandling.

”En klinisk prövning kan ju bli helt förstörd. (...) Då har vi investerat några miljoner, så affärsmässigt kan det ha ganska stora konsekvenser.”

En annan risk var konsekvenser som driftstörning för vårdverksamheten om en tjänst slås ut, vilket i förlängning kan leda till risk för patientskada. Även inverkan på rykte och tillit från såväl vården som slutanvändare togs upp. För verksamheter i ett tidigt skede ansågs den viktigaste tillgången inom företaget vara IP och eventuella patent.

”Just den biten är väl den viktigaste för att vi ska ha något existensberättigande – att vi har försprång med våra idéer och att de inte läcker ut.”

TEMA 3: HINDER FÖR ATT ARBETA MED SÄKERHET

I intervjuerna framkommer att förståelse från ledningens sida är viktigt för ett fungerande säkerhetsarbete. När risken för intrång skattas som låg, kan det vara svårt att prioritera rätt åtgärder och förespråka dem för ledningen. Man lyfter begränsade resurser, både vad gäller personal och ekonomi.

”Det är ju liksom en prioriteringsfråga. Jag menar, vi har andra saker som har varit mer pressande. Kanske hade det varit annorlunda om vi känt att vi varit targetade på något sätt...”

Just att prioritera kostnadseffektiva åtgärder är viktigt för små verksamheter med begränsad budget. Men för företag som generellt har en medicinsk utgångspunkt finns inte alltid kunskapen internt. Externa konsulter eller partners kan komma med förslag men att utvärdera vilka som är nödvändiga och vad som är överflödigt uppfattas som en utmaning.

Ett annat hinder är motstånd från anställda och slutanvändare, eftersom säkerhetsåtgärder kan påverka användarvänligheten.

”Vi använder Onedrive som är en del av Office 365-paketet, men det är en ganska stor mängd säkerhetsfunktioner pålagda där och blir det för krångligt börjar folk använda en privat Dropbox, typ.”

Andra vittnar om att det är svårt att ställa krav på konsulters säkerhetsåtgärder.

60%

av cheferna saknar strategi för cybersäkerhet

Bara fyra av tio chefer i Sverige menar att deras organisation har en strategi för arbetet med cybersäkerhet och färre än hälften uppger att det på deras arbetsplatser finns tydliga regler för de anställda gällande cybersäkerhet.

KÄLLA: Ledarnas rapport Framtiden efter det nya normala 2022.

TEMA 4: ÅTGÄRDER MOT CYBERHOT

Temat berör de tekniska och organisatoriska åtgärder som företag har vidtagit för att motverka de risker som man har identifierat. Främst var det externa konsulter som erbjöd rådgivning. Tekniska åtgärder för att begränsa åtkomst var exempelvis brandväggar, VPN, multifaktorautentisering och systemhärdning för att minska angreppsytan för apparater som står ute i vården. För att minska konsekvenserna av ett intrång nämndes backups för system, dataåterställning samt kryptering.Att separera insamlade hälsodata från personuppgifter var också ett sätt att säkerställa att dessa inte kan kopplas samman vid en eventuell datastöld.

När det gällde personalutbildning varierade denna. Inom mindre företag ansåg vissa att det inte var nödvändigt, då man upplevde att medarbetarna hade tillräcklig kunskap om säkerhetsfrågor. Andra använde en workshop eller heldag med expert inom ämnet. Vid större företag ställdes högre krav på personalens kunskaper. Det kan exempelvis vara en obligatorisk quiz i webbportalen, eller via simulerade nätfiskemail eller andra attacker.

Majoriteten av de intervjuade företagen valde att certifiera sig mot standarden ISO 13485. Den standard som oftast nämndes var ISO 27001, men ingen av de intervjuade hade ännu valt att certifiera sig enligt denna.

”Jag pratar med en del som certifierar sig mot it-säkerhetsstandarder och det jag hör är att de är jättejobbiga, så att certifiera sig det gör man inte med vår typ av företag. Däremot kan man ju använda valda delar av standarden såsom 27 000.”

Enligt studien saknade en väsentlig del av de intervjuade företagen en utarbetad plan för ett intrång eller en incident och ett flertal hade inte heller säkerställt att en systemåterställning var möjlig med de back-ups man hade. Anledningen var att ansvar för IT-miljö och drift lagt ut på tredje part, eller att säkerhetsarbetet inte nått dit.

Många företag brister när det gäller incidenthantering och hela 84 procent hade inte upprättat en plan för vem som ska göra vad vid en cyberattack. Av de drygt 1 200 tillfrågade företagen svarade också 78 procent nej på om de hade en policy för hur man ska agera vid misstanke om brott från inkommande e-post, mess eller telefonsamtal.

KÄLLA: Företagarnas rapport Är det it-säkert? oktober 2022.

84%

saknar plan vid cyberattack

TEMA 5: MOTIVATION FÖR ATT ARBETA MED FRÅGAN

Det femte identifierade temat berör incitament att investera i säkerhet. Här var det extern kravställning som låg bakom ökad investering i informationssäkerhet.

”Det är främst lagstiftning, skulle jag nog säga. Men också att det är något som sjukhusen tittar på, att man är certifierad mot de regelverk som finns.”

För börsnoterade företag eller företag på väg mot börsnotering anses informationssäkerhet bli en mer väsentlig faktor när ett företag ska utvärderas av investerare. Någon gav exempel på att dålig informationssäkerhet kan vara en nackdel vid upphandling.

”Det var en upphandling för inte så länge sen och då var det som bäddat för en aktör, men de förlorade på grund av hur de hanterade information så det gick till en annan aktör istället. Så jag tror att det börjar bli en central fråga.”

Denna uppfattning motiverade vissa att arbeta mot certifiering, exempelvis 27 001. Ytterligare en motiverande faktor är om media rapporterar om incidenter och intrång.

1/3

bara 1/3 av små företag är oroliga för säkerhetsintrång

En motiverande faktor skulle kunna vara oro, men småföretagare är generellt sett mindre säkerhetsmedvetna – bara en tredjedel av småföretagen är oroliga för dataintrång, jämfört med nästan dubbelt så många bland större företag. Mest orolig är man för att datorer eller annan IT-utrustning ska sluta fungera.

KÄLLA: Telias Digitala Index 2022.

TEMA 6: KRAV FRÅN OMVÄRLDEN

Temat berör uppfattningen om vilka krav som bör ställas och hur dessa bör se ut, samt tankar och funderingar kring nuvarande krav.

Omställningen till det nya regelverket såg många företag som en stor utmaning, som skulle innebära betydande kostnader och vara resurskrävande för mindre verksamheter. Även om man ansåg att det var rimligt med något slags kravställning kring informationssäkerhet, fanns åsikten att lagstiftningen innehåller krav som är ovidkommande eller irrelevanta för den egna produkten eller tjänsten.

”Man kan ju ibland tycka att de här cybersecurity-regelverken är väldigt omfattande och tar höjd för allt liksom, för produkter som används i hemmet. Och sen finns det produkter som vår, som står inne i ett sjukhuslab, som kanske inte skulle behöva ha lika strikta krav.”

Några lyfte även att certifieringsprocessen kräver ett anmält organ för att utvärdera produkten. Då dessa är få utgör detta en tidsmässig ”flaskhals”.

Man nämnde även att kravställningen sätter stopp för en mer flexibel utvecklingsprocess vid mjukvaruutveckling. Exempelvis beskrivs agil utveckling inte vara kompatibel med kravställningen. Här nämndes även oro för att medicintekniska produkter behöver lämna marknaden då de inte erhållit certifiering.

Man upplevde också en diskrepans gällande de krav som ställs från olika vårdgivare samt att det ofta är lite ”luddigt” vad som efterfrågas.

Läkemedelsverket välkomnar skärpta krav

Inte helt oväntat skiljer sig bilden åt när en representant för Läkemedelsverket intervjuas. Här tycker man tvärtom att de nya regelverken är rimliga och nödvändiga för att lyfta nivån inom branschen, exempelvis vad gäller riskanalys.

”Många medicintekniska produkter måste verkligen bli bättre på riskanalys, grundorsaksanalys så man verkligen förstår vad som gick fel och inte bara rätta just det här felet – sen händer samma sak en månad senare för att man inte gjort sin hemläxa ordentligt…”

En utmaning i de nya regelverket är att tydliggöra för tjänster att de innefattas av lagstiftningen, exempelvis att programvara faller in i riskklass II:a som i sin tur kräver utvärdering av anmält organ.

Läkemedelsverket lyfte också vikten av att dokumentering och införandet av ett kvalitetsledningssystem sker tidigt i verksamheten, då det förenklar för alla parter. Samtidigt uppmärksammades det att arbetet är ganska omfattande för små verksamheter, men säkerheten inom produkterna bör man inte kompromissa med.

Man ska inte lätta på kraven för dem för det är trots allt rätt riskabla saker de arbetar med, utan snarare hjälpa dem att uppnå kraven. Istället bör mindre verksamheter kunna erbjudas regulatoriskt stöd, exempelvis via inkubatorer som i dag ger råd om andra delar i verksamheten.

Olika mognad i olika regioner

Från regionens sida efterlystes kollektivt ansvar från vården, som i rollen av upphandlare bör driva utvecklingen i rätt och samma riktning. Man beskriver att det blir en avvägning mellan cybersäkerhet å ena sidan och att alls få tillgång till medicinteknik å den andra.

”Om man ska generalisera är det en ganska dålig mognad vad gäller cybersäkerhet och informationssäkerhet i de här produkterna. Det blir en konstant avvägning då på vilka krav vi kan ställa dem och hur, för att inte utesluta och landa i en verklighet där vi inte får in någon utrustning alls.”

Mognaden har heller inte varit på samma nivå bland alla vårdgivare. Exempelvis kan en region köpa in och implementera en produkt, som en annan region senare finner vara problematisk att införa på grund av cybersäkerhetsbrister.

En förhoppning från regionen var att det nya regelverket skulle höja standarden. Ett förslag som lyftes var en samordnande funktion eller myndighet.

Inom sjukvården finns även krav på patientdatalagen, som företag generellt inte måste förhålla sig till.

Regionen höll med Läkemedelsverket om att dataskyddsfrågor och informationssäkerhetsfrågor kommer in för sent i processen, när företagen redan tycker sig vara mogna att gå in på marknaden.

> Man ska inte lätta på kraven för dem, det är trots allt rätt riskabla saker de arbetar med, utan snarare hjälpa dem att uppnå kraven.
>
> Livsmedelsverket

> Det blir en konstant avvägning på vilka krav vi kan ställa och hur, för att inte utesluta och landa i en verklighet där vi inte får in någon utrustning alls.
>
> Regionen

TEMA 7: DIGITALISERING I VÅRDEN GENERELLT

Här var respondenterna generellt eniga om att det fanns en stor potential att förbättra vården, men flera upplevde att omställningen går för långsamt för att möta kommande behov. Men det fanns en kluvenhet, då man samtidigt såg risker med att det gick för fort.

Några beskriver motstånd mot att integrera lösningar eftersom ansvaret blir svårare att fastställa när processer som tidigare var i vårdgivarens kontroll blir automatiserade. En risk som framhålls är att vården flyttar till hemmet och bristande förmågan att då erbjuda vård om driften av dessa tjänster av något skäl skulle slås ut eller vara otillgängliga.

En utmaning många ser framför sig gäller integreringen av en mängd olika system vilket innebär en komplex angreppsyta som är svår att kartlägga. Här efterlyste man ett holistiskt synsätt, istället för individuell utvärdering av alla delar.

En förändring som efterfrågades var en övergång till öppna journalsystem utifrån en gemensam standard, där exempelvis openEHR nämndes.

Intervjudeltagarna ser olika problem, där en företagare menar att den offentliga upphandlingsprocessen har en hämmande effekt på utvecklingen inom sektorn:

”Det är ju en jättemödosam process, vi får lägga ner massa tid på en sådan upphandling. Då kan vi kanske göra något vettigare med den tiden och kanske hellre vinna ett projekt med en privat vårdgivare.”

Viktigt att ta hänsyn till den digitala miljön

Från Läkemedelsverkets sida betonade man vikten av ett aktivt samspel mellan leverantörer som verkar i samma miljö och att dessa beaktar vilka system man samverkar med.

”Ofta tar man bara ansvar för sin del och säger att resten släpper jag. Då missar man regelverkets krav på att man ska ta hänsyn till miljön som det här ska finnas i. Då måste jag ta hänsyn till andra programvaror som finns där och kanske fundera kring att man har ett tydligt avtal. Säg att du har två programvaror som kopplar upp sig mot varandra och sen uppdaterar den ena utan att tala om det, då kan det gå väldigt illa.”

Läkemedelsverket uppmärksammade även risken som vård i hemmet medför för patienten om infrastrukturen av något skäl skulle slås ut. Mister man övervakningen går det inte att veta om patienten exempelvis får sin medicin eller drabbas av försämring.

Driftstörningar problem vid vård på distans

Även de intervjuade från regionen framhävde utmaningen med att erbjuda vård på distans om de digitala system man förlitar sig på stöter på en driftstörning.

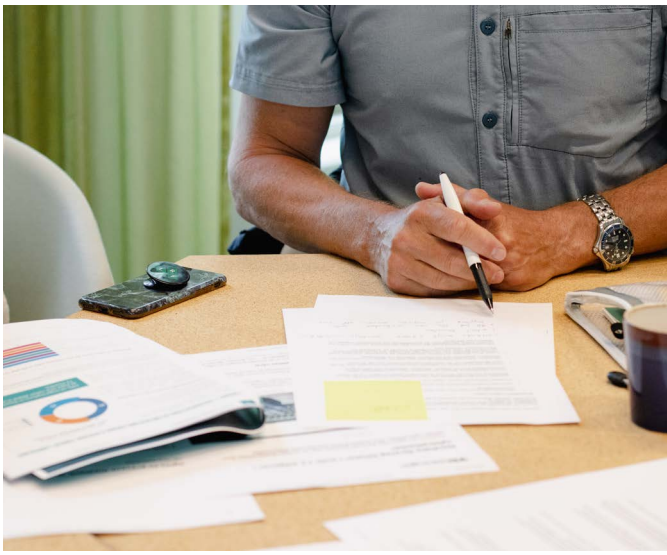
”Det finns besparingsmöjligheter i exempelvis hemsjukvård, men får man störningar krävs förutsättningar att hantera det på något alternativt sätt – har man jobbat bort personalresurser är det svårt att lösa det på något annat sätt än digitalt.”

Även sjukhusvård betraktas som mer beroende av digitala tjänster och förmågan att här återgå till äldre arbetssätt är begränsad. Men betonar också att en del kontroll går förlorad i takt med att vården är decentraliserad och beroende av tjänster som vården inte själv förfogar över.

7 STUDIENS RESULTAT

Frågeställningen som studien utgick ifrån var: Hur arbetar medtechföretag för att motverka risker och hot inom cybersäkerhet?

Bland de intervjuade små och medelstora företagen bedömdes risken för intrång i verksamheten vara låg, varför man satsade mer på att investera i informationssäkerhet i den tjänst eller produkt som verksamheten erbjuder.



Intervjuerna utfördes inför att nya förordningar som ställer strängare krav på patientsäkerhet samt cybersäkerhet för medicintekniska produkter ska införas. Kraven som dessa ställer, samt krav från vården, utgjorde den primära motivationen för företagen att investera i informationssäkerhet.

Ett flertal intervjuade företagare var kritiska mot de nya regelverken och menade att arbetet som krävs för att uppnå kraven är alltför omfattande för mindre företag.

Här skiljer sig dock åsikterna åt mellan företagen och Läkemedelsverket samt regionen – de båda sistnämnda betraktade tvärtom de kommande, skärpta kraven som både rimliga och nödvändiga.

Det fanns en samsyn hos alla om att cybersäkerhet är ett viktigt område. Man var även eniga om att det finns behov av ökat stöd för små och medelstora verksamheter för att kunna uppnå de krav som ställs, samt av ökad dialog mellan de olika aktörerna.

Framtida studier

En förhoppning är, enligt examensarbetets författare, att studien kan ligga till grund för en mer omfattande kartläggning. Ett komplement skulle då kunna vara att även inkludera anmälda organ som är ansvariga för den fortsatta utvärderingen av medicintekniska produkter samt utdelning av CE-märkning. En annan relevant aktör är Inspektionen för vård och omsorg, IVO, som tillsammans med Läkemedelsverket ansvarar för tillsynen av medicintekniska produkter. En kompletterande, kvantitativ studie skulle också vara av intresse för att bredare fånga upp hur branschen ser på cybersäkerhet.

RESULTATEN I SJU PUNKTER:

1) Risker: Generellt upplevde företagen att risken för en attack mot verksamheten var låg på grund av låg synlighet och verksamhetens ringa storlek. Mer påtagliga ansågs risken vara för uppkopplade apparater och tjänster. Exempelvis uppfattas tjänster som används direkt av konsumenter eller ansluter till vården ha högre risk för intrång. Oftast nämndes nätfiske och ransomware som specifika hot.

2) Följder: Här nämndes förlust av IP, läckage av personuppgifter, inverkan på rykte från vården och slutanvändare, sabotage av pågående kliniska studier samt driftstörning för vården om tjänsten skulle slås ut.

3) Hinder: Många av företagen har svårt att prioritera rätt åtgärder samt att förespråka dessa. Det beror på att risken för intrång i verksamheten anses vara låg och att verksamhetens resurser är begränsade. Mycket av arbetet sköttes av externa konsulter och att ställa krav på dessa uppfattades som en utmaning.

4) Åtgärder: De flesta företag hade vidtagit åtgärder för att förhindra intrång och för att motverka eventuella konsekvenser, exempelvis genom backups eller separation av personliga och medicinska data. En åtgärd som ofta saknades var en utarbetad plan vid ett eventuellt intrång eller attack på verksamheten. För att höja säkerheten användes ett antal standarder, där den vanligaste var ISO 13485 för stöd i framtagandet av ett kvalitetshanteringssystem samt ISO 27000-serien.

5) Motivation: Incitament för att förbättra informationssäkerheten kommer från externa källor som regelverk, från vårdens krav samt från eventuella investerare där informationssäkerhet uppfattas som en central fråga.

6) Kravställning: De kommande regelverken uppfattades som ett hinder, som medför stora kostnader och stor arbetsbörda för mindre verksamheter. Många intervjuade menar att eftersom en stor mängd olika medicintekniska produkter inkluderas är mycket av kravställningen alltför generell och kanske inte alls nödvändig för den typ av produkt som verksamheten erbjuder.

Både vårdgivare och Läkemedelsverket ansåg att informationssäkerheten behövde förbättras hos medicintekniska företag och hoppas att regelverken kommer att höja standarden.

Vården har ibland fått göra kompromisser avseende informationssäkerhet, eftersom marknaden inte uppfyller kraven. Intervjuade från företag och region upplevde att kravställningen i offentliga upphandlingar varierar mycket från vårdgivare till vårdgivare. Det gör det svårt för leverantörer att veta vilka åtgärder som är värda att investera i, vilket kan minska motivationen att förbättra informationssäkerheten.

7) Digitalisering: Här nämndes tre primära utmaningar:

• Det ökade beroendet av de digitala verktyg man använder och svårigheten att återgå till äldre arbetsmetoder.

• Ett ökat beroende av infrastruktur utanför vårdens kontroll för en vård som i allt större utsträckning sker på distans.

• Samkörandet av olika system och hur dessa ska integreras och avgränsas på bästa sätt. Här menar flera att det krävs mer samspel mellan olika aktörer – som vård, leverantör och myndighet, samt att mer tankemöda måste läggas på i vilken miljö som produkten är tänkt användas i.

En fjärde utmaning är bristen på anmälda organ som gör att en stor andel av de medicintekniska produkter som erbjuds idag riskerar att lämna marknaden.

8 VAD KAN FÖRETAGEN GÖRA?

I studien vittnar intervjuade om att det är svårt att få gehör från ledningen när det gäller att arbeta med informations- och cybersäkerhet.

Marianne Rilde Björkman är senior specialist inom informations- och cybersäkerhet med lång erfarenhet från bland annat Praktikertjänst och nu senast från Myndigheten för samhällsskydd och beredskap, MSB. Rimmar det ovanstående med hennes erfarenheter?

– Svar ja! Generellt är förebyggande arbete oftast svårt att få ledningen att satsa på, då det inte självklart går att se nyttan. Tvärtom vill man arbeta med utvecklingen av sin produkt och få ut den på marknaden, säger hon.

De nya regelverk som beskrivs i kapitel 5 är snåriga och hon menar att i ett mindre företag vet man inte vem man ska vända sig till och hur ens eget arbete ska kunna anpassas. Samtidigt behöver regelverken uppdateras, anser hon.

– Jag kanske sticker ut hakan, men när det gäller NIS2 så behöver det ställas ökade krav. NIS2 behövs för att vi ska ha en samsyn och liknande krav inom hela EU. Exempelvis är det viktigt att kunna riskbedöma underleverantörer och produkten under hela produktionskedjan och livscykeln, säger Marianne Rilde Björkman.

Företagen har svårt att se nyttan

I studien gick det även att se att det främst var externa krav, som lagstiftning eller krav från vården, som anfördes som skäl för att arbeta med informations- och cybersäkerhet.

– Man förstår inte riktigt vad som konkret ska göras i företaget och då har man svårt att se nyttan för det egna företaget. Drivkraften blir då att uppnå lagkrav, istället för att man har drivkraften att arbeta med frågan för att uppnå konkurrensfördelar, säger hon.

Även detta har Marianne Rilde Björkman sett förut, exempelvis vid införande av kvalitetsledningssystem på Praktikertjänst.

– Många inom vården tyckte det var ett jobbigt krav uppifrån. Bara några få såg möjligheten att själva få mer ordning och reda och faktiskt öka sin lönsamhet på sikt, säger hon.

Hon tror dock att det kommer att gå snabbare att få företagen att förstå vikten av informations- och cybersäkerhet, än vad som var fallet vid exempelvis införandet av miljökrav.

– Miljökrav innebär merarbete och även om det känns bra att göra världen bättre avspeglas inte alltid nyttan direkt i den egna verksamheten. Cybersäkerhet tror jag kan gå snabbare att förstå verksamhetsnyttan med när man inser att ”herregud - jag riskerar att bli av med data och immateriella värden om vi drabbas av ett avbrott i verksamheten genom exempelvis en attack!”, säger hon.

Avvägning mellan säkerhet och patientnytta

Något som också framkom i studien var ett slags ”etiskt dilemma” för vården. Intervjuade representanter från en region menade att de kunde behöva ge avkall på informations- och cybersäkerhet för att inte utesluta leverantörer och riskera att inte få tillgång till någon utrustning alls – en avvägning mellan informationssäkerhet och patientnytta. Även detta känner Marianne Rilde Björkman igen från sin tid på MSB. Där gjordes för fem år sedan en genomgång av regionernas informationssäkerhet och myndigheten besökte senare 18 av 21 regioner.

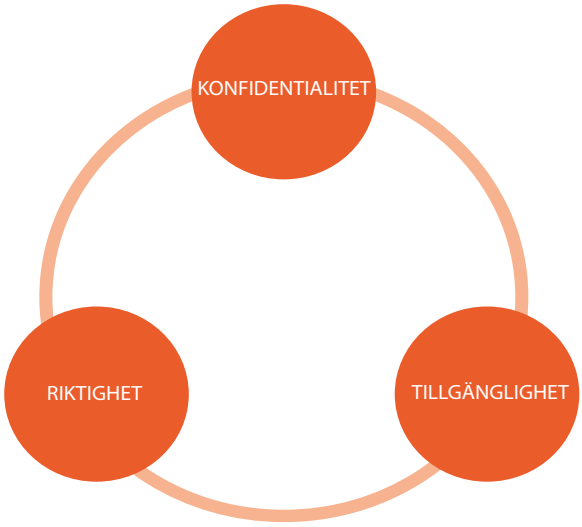
– Här kunde vi konstatera att generellt var medicinteknik ett svårt område, som ett svart hål. Man menade att man var i beroendeställning till de som tillverkat utrustningen och som bestämde hur informationen skulle hanteras och lagras, säger hon.

I rapporten En bild av landstingens säkerhetsarbete 2018: kartläggning och analys av landstingens informationssäkerhetsarbete inom hälso- och sjukvården beskriver de att just vad gällde medicinteknik hamnade säkerheten i en gråzon.

Hon menar att ett problem också kan vara att man ser cybersäkerhet som enbart en it-fråga, som it-avdelningen ska ha hand om, när det egentligen handlar om en informationssäkerhetsfråga. För att bibehålla informationssäkerheten behöver man säkerställa informationens konfidentialitet, riktighet och tillgänglighet, KRT.

Riktighet är otroligt viktigt. Marianne Rilde Björkman exemplifierar med om någon i journalsystemet byter ut informationen om patienters blodgrupper.

– Det kan dels vara svårt att upptäcka, dels helt livsfarligt för patientsäkerheten och ofta svåra att åtgärda, säger hon



Konfidentialitet betyder att informationen är tillgänglig endast för de personer som har behörighet ta del av den.

Riktighet betyder att innehållet i informationen ska vara korrekt och inte kunna förändras av obehöriga.

Tillgänglighet betyder att informationen ska vara nåbar när den behövs.

På engelska är begreppet CIA för confidentiality, integrity, availability.

Önskemål om bättre samverkan och stöd

I studien efterlyste de intervjuade bättre samverkan mellan vårdgivare, leverantör och tillsynsmyndighet och även strukturerat stöd till små och medelstora företag inom medicinteknikbranschen.

– Nationellt satsas mycket på start-ups, men sedan finns saknas fortsatt stöd, exempelvis plattformar för att testa teknik eller stöd i att möta de nya och striktare regelverk som kommer från EU. Här skulle det behövas nya mötesrum, säger Marianne Rilde Björkman.

En hake är att vården styrs i 21 olika regioner med olika slags datasystem.

– Men om det vore möjligt för dem att gemensamt ställa krav vad gäller cyber- och informationssäkerhet skulle det underlätta för leverantörerna, säger hon.

Socialstyrelsen är sedan den 1 oktober 2022 sektorsansvarig myndighet inom hälsa, vård och omsorg.

– De skulle kunna ta ledningen i samverkansarbetet och hur man ska utforma det efterfrågade stödet och verka ihop med andra, säger Marianne Rilde Björkman.

Här nämner hon Inera AB som är kommunernas- och regionernas digitaliseringsbolag, samt MSB.

Stora hot mot små och medelstora företag

Något som var tydligt i studien var att de små och medelstora företagen inom medicinteknikbranschen inte såg sig som så utsatta, något som inte stämmer.

– När det gäller medicinteknik agerar stora leverantörer på en global marknad och hittar man en bakdörr in i ett system så går ju den att använda oavsett i vilket land apparaten finns, säger hon.

I mars i år gjorde en cyberattack att trygghetslarm för äldre slogs ut i nära hälften av alla kommuner, där vissa larm inte fungerade under nästan ett helt ett dygn.

– Medicinteknik är en unik bransch eftersom liv står på spel. Att ett tillverkande företag drabbas av stopp i produktionen kostar visserligen pengar, men här har vi en situation som kan leda till dödsfall, säger hon.

Företagare fick riktad säkerhetsutbildning

Ett grundläggande steg för att företag ska arbeta med informations- och cybersäkerhet är utbildning i frågan. Under 2023 har Marianne Rilde Björkman lett programträffarna i ett numera avslutat projekt. Målgruppen var små och medelstora företag i olika stadier av mognad.

– Säkerhetsarbetet är viktigt i alla skeden, men just för start-ups och scale-ups har man chansen att bygga rätt från början, vilket ju är en stor fördel, säger hon.

Under fem halvdagar fick deltagarna kunskap och verktyg för att börja införa ett grundläggande och konkret systematiskt informations- och cybersäkerhetsarbete, som till stor del motsvarar kraven i exempelvis NIS2.

– Många uppfattar att ISO27001 är otydligt, men att få igång ett konkret informationssäkerhetsarbete är precis det vi gör här i programmet, säger hon.

På den sista träffen iscensätter man en cyberattack i form av ett rollspel.

– Det som gladde mig mycket var att deltagarna har gått från ord till handling. Att förstå att man behöver vidta åtgärder är en sak, men att förändra sitt beteende och skapa bra arbetssätt är något helt annat, säger hon.

Ledningen måste fatta aktiva beslut

Att driva företag innebär alltid att ta olika risker, men Marianne Rilde Björkman menar att

ledningen och styrelser behöver mer aktiva i att fatta medvetna beslut vad gäller informations- och cybersäkerhet.

– De behöver också förstå att detta inte bara är en it-fråga, utan att det handlar om den information som behövs för att verksamheten ska fungera, säger Marianne Rilde Björkman.

Hon menar att man är mycket kunniga vad gäller regelverk för sin specifika produkt, men man har inte samma insikt om de regelverk som gäller själva verksamheten.

– Medicinteknik kan, om informations- och cybersäkerhetsarbetet kommer på plats, bli en stor och viktig exportvara för Sverige, då vi ligger långt fram både vad gäller digitalisering och innovation, säger hon.

”Allt handlar inte om cyberhot”

Det viktigaste är, enligt henne, att öka medvetenheten och höja kunskapsnivån.

– Frågan om informations- och cybersäkerhetmåste upp på bordet! Vi behöver våga prata om att attacker även drabbar mindre företag. Man behöver också vara medveten om att många incidenter sker genom handhavandefel eller att vi gör misstag i arbetet, så allt handlar inte om cyberhot, säger hon och fortsätter:

– Inom medicinteknikbranschen behöver man nätverka och hjälpa varandra, istället för att bara se varandra som konkurrenter. Det var tydligt i pilotprojektet att deltagarna uppskattade att kunna diskutera med varandra och känna att man inte stod ensam.

Att medarbetare har god teknisk kompetens, betyder inte nödvändigtvis att man har tillräcklig kunskap inom informationssäkerhet.

– Här finns risken att medicinteknikföretag invaggas i falsk trygghet, säger hon.

Hon listar några åtgärder som alla företag inom medicinteknikbranschen bör fundera över (se ruta). Framförallt den sista punkten.

– Det är inte frågan om det kommer att hända utan när, så se till att ha en strategi för hur ni ska handla då, säger hon.

Att medvetandegöra och utbilda medarbetarna är en grundläggande del.

> Kultur vinner alltid över struktur, så det är extremt viktigt att bygga en bra säkerhetskultur inom företaget.
>
> Marianne Rilde Björkman

– Kultur vinner alltid över struktur, så det är extremt viktigt att bygga en bra säkerhetskultur inom företaget, säger Marianne Rilde Björkman.

SÅ KAN DITT FÖRETAG FÖRBEREDA SIG:

• Inventera din viktiga information – är det patientinformation, företagsinformation, immateriella rättigheter, patent eller annat?

• Identifiera och bedöm verksamhetens risker.

• Välj ut vilka säkerhetsåtgärder som informationen behöver för att ge rätt skydd.

• Medvetandegör medarbetarna för att begränsa misstag via den mänskliga faktorn.

• Förbered dig på det värsta och utarbeta en plan: vad gör vi när vi – antingen via egna misstag eller en utomstående attack – förlorar kontrollen över viktig information?

• Och det är absolut avgörande att ha bra rutiner för back-up, testa att återläsa dem och förvara dem säkert.

HÄR FINNS MER INFORMATION OM CYBERSÄKERHET

Läs mer på MSBS hemsida: www.msb.se och www.informationssäkerhet.se

Inom EU är det cybersäkerhetsorganisationen ENISA som har hand om frågan, se mer information här: www.enisa.europa.eu

9 REFERENSER

Källorna sorteras per kapitel och listas här i den ordning de använts i texten.

Kapitel 4:

Healthcare Cybersecurity: The Biggest Stats and Trends in 2023. Safety Detectives.

Är det it-säkert? Företagarnas rapport från oktober 2022.

Cybersäkerhet i Sverige 2022. Del 1: Hot, metoder och beroenden. Nationellt cybersäkerhetscentrum.

Regeringens styrning av samhällets informations- och cybersäkerhet – både brådskande och viktig (RiR 2023:8) från april 2023.

Telias Digitala Index 2022.

Cyberbrott mot svenska företag – hur bygger vi en säkrare framtid? Stockholms Handelskammares rapport från juni 2022.

Medtech Cyber-Incidents: A Costlier Problem Than You Think, Med Device Online, 17 augusti 2022.

Kapitel 5:

Säker digitalisering inom medtech: Hur arbetar medtechföretag för att motverka risker och hot inom cybersäkerhet? Examensarbete av Angus Bergman.

NCS3 – Patient- och cybersäkerhet rörande medicintekniska produkter. En NCS3-studie om avvikelserapportering och CE-märkning. Rapport från FOI beställd av MSB, december 2021.

Nya säkerhetslagen snart här – men svenska företag är inte på banan. Karin Lindström, IDG.se, 28 februari 2023.

Kapitel 6 och 7:

Säker digitalisering inom medtech: Hur arbetar medtechföretag för att motverka risker och hot inom cybersäkerhet? Examensarbete av Angus Bergman.

Telias Digitala Index 2022. Framtiden efter det nya normala Ledarnas rapport från 2022.

Är det it-säkert? Företagarnas rapport från oktober 2022.

Kapitel 8:

Texten baseras huvudsakligen på intervju med Marianne Rilde Björkman, säkerhetsspecialist.