SÄKER DIGITALISERING I BESÖKSNÄRINGEN

RAPPORTEN BESTÄLLD AV

tillväxtverket

Region Östergötland

LINKÖPING SCIENCE PARK

SAMMANFATTNING

I en bransch som besöksnäringen där alltmer av verksamheterna digitaliseras tillkommer ett behov av att ha kunskap kring den digitala säkerheten och de risker och hot som finns. Besöksnäringen digitaliseras allt mer med nätverk, hemsidor och digitala boknings- och kassasystem. Detta dels för att minska det administrativa arbetet och få smidigare, effektivare verksamheter, dels för att öka marknadsföringen av företaget och bredda erbjudandet till kunder. Med digitaliseringen introduceras dock även risker och hot vilka kan leda till att verksamheterna kan skadas exempelvis om data läcker ut eller system ligger nere vilket kan medföra att också verksamheten tillfälligt inte kan bedrivas. Den digitala mognaden i besöksnäringen är generellt låg, företagen är vanligen små verksamheter med begränsade resurser och därmed även begränsad kunskap kring IT-säkerhet.

Kartläggningen undersöker behovet av och inställningen till digitalisering och digital säkerhet hos små till medelstora företag i besöksnäringen. 32 företag med verksamheter i Östergötland har intervjuats för att få en lägesbild av behovet av ökad kompetens kring IT-säkerhet. Därtill har sex leverantörer av IT-system och lösningar till företag inom besöksnäringen intervjuas för att bredda lägesbilden med fler perspektiv på risker, rutiner och synen på digital säkerhet.

Av undersökningen framkommer det att en stor del av bolagen i besöksnäringen är familjeföretag, där ägarna ofta arbetar operativt i den dagliga verksamheten. Således finns sällan en specifik roll för IT och IT-säkerhet, utan dessa frågor ansvarar vanligen ägarna för. Verksamheterna är generellt små, och resurser att lägga på säkerhetsfrågor saknas, de resurser som finns läggs på att digitalisera verksamheterna genom digitala kassasystem, nätverk och hemsidor. I och med de begränsade resurserna hos de mindre företagen har många gjort delar av digitaliseringen själva eller tagit hjälp av en bekant. Många har exempelvis gjort sin hemsida och satt upp nätverk själva, men saknar kunskap om att driva, underhålla och uppdatera den, och har därmed inte heller kunskap kring säkerhetsaspekter av de digitala verktygen.

De flesta företag i besöksnäringen är medvetna om sin låga IT-kompetens, och är dessutom tydliga med att de gärna skulle öka kunskaperna inom verksamheten. Då både ägare och medarbetare ofta arbetar operativt i den dagliga verksamheten samtidigt som verksamheterna är små med begränsade resurser, har man dock inte möjlighet att lägga resurser på att skaffa sig mer kunskap och kompetens. Detta leder till att företagen saknar kompetens kring vad man köper in och vad man kan ställa för krav på leverantörerna.

Företagen i besöksnäringen har visat sig ha svårt att utvärdera de digitala tjänster som köps in ur säkerhetssynpunkt, och säkerhet är inte heller något som prioriteras vid upphandlingar. Företagen uttrycker att man har stor tillit till leverantörerna, men vet egentligen inte särskilt mycket om hur uppdelningen av ansvar ser ut gentemot leverantörerna. Från leverantörernas sida är det tydligt att storleken på företagen spelar stor roll för hur mycket krav kunderna ställer. De kan se att ju större kunden är, desto fler säkerhetsrelaterade krav ställer de. Enligt leverantörerna är det dock få som ställer krav på, eller intresserar sig för en diskussion kring säkerhetsfrågor. Även hos de allra största kunderna är intresset lågt och kommunikationen med leverantörerna kring IT-säkerhet nästan obefintlig.

Innehållsförteckning

1.	Introduktion	6
2.	Arbetsgång	7
3.	Bakgrund	7
Besöksnäringen		7
Digitalisering i besöksnäringen		8
Digital säkerhet		10
Risker för företag i besöksnäringen		10
Aktörer och incitament		13
Sårbarheter		14
Digitala angrepp i besöksnäringen		14
Digital mognad och riskhantering		17
Säkerhetscertifikationer och säkerhetsramverk		19
Digitalisering och IT-säkerhet hos företag i besöksnäringen		19
Digitala verktyg och system		19
Risker och hot kopplat till de digitala verktygen i besöksnäringen		22
Rutiner, policys och riskanalyser		22
Risker för verksamheterna		23
Risker med hemsida, nätverk och behörighet		25
Förhållande till leverantörer		25
Utmärkande likheter och skillnader		25
IT-leverantörer inom besöksnäringen		27
Erbjudande		27
IT-säkerhet		28
Besöksnäringen ur leverantörernas perspektiv		30
Synen på ansvar		30
Slutsatser		31
Digitala verktyg och kompetens		32
Synen på digital säkerhet		32
Hot och risker		33
Framtidsutsikter		33
Litteraturförteckning		34
Beställarnas kommentarer		36

Introduktion

Besöksnäringen är en bransch där företag i allt större utsträckning digitaliserar mer av sin verksamhet, där digitala boknings- och kassasystem, hemsidor och nätverk för gäster blir vanligare. Besöksnäringen kännetecknas av mindre bolag med verksamheter inom livsstil och upplevelser, där verksamheten vanligen är säsongsstyrd med ökad aktivitet under sommarhalvåret. Den pågående digitala utvecklingen hos dessa företag underlättar för intern kommunikation och arbete inom verksamheten, ökar tillgängligheten och breddar erbjudandet till besökare och kunder. Även om digitaliseringen ökar är branschens digitala mognad fortfarande låg, och digitalisering av verksamheterna medför även en introduktion av nya hot och risker, där en attack mot företagets IT-miljö kan medföra stora ekonomiska och organisatoriska konsekvenser.

I denna branschrapport ges en introduktion till vad säker digitalisering i besöksnäringen innebär; inledningsvis en övergripande beskrivning av besöksnäringen och därefter introduktion till olika IT-relaterade hot och risker samt vilka aktörer som kan ha incitament att utföra angrepp. Efter denna bakgrundsbeskrivning presenteras en lägesbeskrivning av IT-säkerheten hos verksamheter i besöksnäringen. Lägesbeskrivningen baseras på 32 intervjuer med representanter från företag i besöksnäringen i Östergötland, allt från nationella kedjor till enpersonsföretag, där olika verksamhetstyper inom besöksnäringen finns representerade. För att ytterligare nyansera nuläget för digitalisering och digital säkerhet i branschen hämtas information även från leverantörer av digitala system till besöksnäringen, för att ge en bild av hur dessa aktörer ser på och arbetar med säkerhet.

Det övergripande syftet med branschrapporten är att kartlägga vilka digitala verktyg som används inom besöksnäringen, samt hot och risker kopplade till dessa. Detta för att ge en bild av nuläget inom branschen och vidare kunna resonera kring framtidsutsikter i form av förbättringsområden och strategiska arbetsområden. Besöksnäringen är en av de branscher som använder sig minst av IT-säkerhetsåtgärder och där behovet av

medvetenhet kring hotbilder och risker är stort [1]. En branschrapport med en kartläggning av nuläget för digital säkerhet är ett första steg i ett projekt som på sikt ska genomföra insatser för att höja den digitala kompetensen hos företag inom besöksnäringen.

Branschrapporten genomförs av Unitalent på uppdrag av Tillväxtverket, Linköpings Science Park och Visit Östergötland och utgår från besöksnäringen i Östergötland. Den är en del av ett större projekt med fokus på digital säkerhet inom besöksnäringen. Baserat på de slutsatser som dras i rapporten kommer en utbildning inom digital säkerhet genomföras i projektet, en utbildning som kommer erbjudas företag i besöksnäringen samt kompletteras med möjlighet till individuellt stöd från IT-säkerhetsexperter. Målsättningen med projektet är att sprida kunskap och professionalisera ledning och styrelser hos företag inom besöksnäringen, för att i större utsträckning kunna arbeta med digitalisering på ett säkert sätt och säkerställa att besöksnäringen bidrar till att skapa ett robust och motståndskraftigt samhälle.

Arbetsgång

Kartläggningen baseras på anonyma intervjuer med representanter från företag inom besöksnäringen i Östergötland, med samtal utifrån frågor om företagens verksamhet, den digitala miljön och olika aspekter av digital säkerhet. Fokus har legat på att få en översiktlig bild av hur företagens verksamhet fungerar, vilka digitala verktyg och system som används, hur data hanteras i dessa och hur företagen själva ser på och arbetar med digital säkerhet.

Övervägande delen av de företag som har intervjuats är små till medelstora verksamheter, med omkring en handfull anställda och en eller ett par ägare. En del av företagen har dock varit små verksamheter med exempelvis ett ägande par som de enda anställda, medan ett fåtal har varit större kedjor med ett huvudkontor, en IT-avdelning och verksamheter runt om i landet.

Intervjuerna baseras enligt semistruktur på ett antal förberedda frågor strukturerade utifrån relevanta områden gällande verksamhetens IT-miljö, rutiner och kunskaper inom IT-säkerhet. Samtalen har sedan till viss del styrts om utifrån respondenternas svar, exempelvis genom att gå in mer och djupare på de frågor där företaget har haft mer att säga och styra om ordningen på resterande frågor för att få ett naturligt flyt i samtalen och samtidigt täcka så mycket som möjligt av de efterfrågade områdena.

För att göra kartläggningen än mer omfattande med fler perspektiv har intervjuer även gjorts med leverantörer av de IT-system som företagen inom besöksnäringen använder sig av. Med utgångspunkt i svar från de tidigare intervjuerna om vilka leverantörer som används av företagen i besöksnäringen togs en lista över leverantörer fram, vilka sedan kontaktades för anonyma intervjuer. Leverantörerna intervjuades bland annat kring deras syn på digital säkerhet intern och gentemot sina kunder, kring ansvarsfördelning när det gäller säkerhet och hur risker och hot de ser för den egna verksamheten och sina kunder.

Intervjuerna med företag respektive leverantörer sammanställs sedan i varsitt avsnitt, där det insamlade materialet struktureras upp under ett antal olika relevanta områden, innan slutsatser och framtidsutsikter dras utifrån intervjuerna och bakgrundsbilden.

Bakgrund

Besöksnäringen

Besöksnäringen är en bransch som inkluderar i princip all konsumtion som är direkt kopplad till resande, från affärsresande och utländska besökare till dagsbesök. Inom besöksnäringen ligger fokus generellt på livsstil där företagen erbjuder upplevelser inom många olika områden som hästturism, måltidsupplevelser, spa, stugut-

hyrning, naturupplevelser, kajakuthyrning eller jakt och fiske. Utmärkande för besöksnäringen är att den kännetecknas av små företag som drivs av ägarnas livsstil, där medarbetare och ägare arbetar operativt i den dagliga verksamheten. Mycket av den verksamhet som bedrivs av företagen är säsongsberoende, de flesta har betydligt fler besökare under sommarhalvåret än resten av året. Branschen kännetecknas av relativt små bolag, med ett par eller en handfull heltidsanställda året runt, och med en utökad personalstyrka under högsäsong.

Något annat som utmärker besöksnäringen gentemot andra branscher är att verksamhetens erbjudande handlar om besökarnas personliga upplevelser; värdeskapande och skapande av personliga upplevelser där kunden står i fokus. Detta gör att företagen inte själva äger upplevelserna de erbjuder, utan att värdet styrs av kundens personliga upplevelse, något som kräver professionellt värdskap och personliga möten. Många företag inom besöksnäringen är därmed personliga, flexibla och anpassningsbara i sin verksamhet, något som ofta är fördelaktigt, men som likväl kan vara en utmaning när det kommer till att ha långsiktiga affärs- och utvecklingsplaner för att kunna möta oförutsedda och omfattande förändringar [2].

Målgruppen och kunderna för företagen inom besöksnäringen är bred och de resande varierar från barnfamiljer och vuxna utan barn till pensionärer och unga vuxna. Förutom att variera i ålder och stadie i livet, har besökarna även olika bakgrund och intresse. Anledningarna till besök varierar därför; det kan vara möjligheten att paddla kajak i skärgården, besök på ett speciellt museum eller ett musikevenemang, att vara på genomresa och i behov av boende för en natt, eller så kan det vara ett kundbesök eller en konferensresa. Gemensamt för företagen i besöksnäringen är att de generellt arbetar med kundnära verksamhet, då kundens upplevelse står i fokus. Det är således viktigt med lättillgänglig information, god kommunikation och tryggt och säkert bemötande.

Digitalisering i besöksnäringen

Enligt Visit Sweden [3] ökar efterfrågan på digital anpassning och tillgänglighet från besökare, och inspiration, informationshämtning, planering, bokning och delande av upplevelser digitalt beskrivs som efterfrågat av resenärer. Digitaliseringen inom turism och besöksnäringen har utvecklats snabbt de senaste åren, och många av företagen i näringen lägger resurser på att digitalisera delar av sin verksamhet med digitala bokningssystem, kassasystem och en hemsida. Region Östergötland [4] beskriver det som en utmaning för besöksnäringen med fortsatt utveckling av dessa digitala system, där fokus ligger på digital tillgänglighet av information, bokning och annat som underlättar verksamheten. Det kan exempelvis göras genom utveckling av lättillgängliga bokningssystem för kunder, säkra kassasystem för verksamheten och användarvänliga och tillgängliga hemsidor med information och kommunikationsmöjligheter.

I och med att det inom besöksnäringen finns många livsstilsföretagare med mindre verksamheter, är behovet av kunskap om att starta, driva och utveckla företag viktig liksom kunskap om de digitala systemen som används. Enligt Regeringen [2] finns behov av kunskap om hur digitala verktyg kan användas och hanteras för att digitalisera, effektivisera och utveckla verksamheterna i besöksnäringen, där kunskap om digital säkerhet är en del. Att nyttja digitaliseringens möjligheter är centralt och kräver både kortsiktig och långsiktig utveckling och kunskap kring de digitala systemen. Digitaliserade system, ny teknik och innovation kan bidra till hållbar utveckling, förenklat företagande och ökad lönsamhet för turistnäringen [2].

I och med besökarnas ökade efterfrågan på digital tillgänglighet finns fördelar med en fortsatt utveckling av och ökad kunskap kring de digitala system som idag används och som framöver kan komma att användas inom besöksnäringen. Bokningssystem är system för att samla, organisera, lagra och hantera bokningar vilket är exempel på ett system som kan medföra positiva följder för verksamheten om det digitaliseras. Genom att

digitalisera bokningssystem kan verksamheten få ett heltäckande system som kräver mindre administration och som kan organisera och samordna olika delar av verksamheten. Ett digitalt bokningssystem är ofta kopplat mot en extern part som exempelvis Booking.com som ger kunder möjlighet att boka inte bara via företaget själva utan även via den externa parten. Detta ger kunderna fler möjligheter och alternativ, och ökar dessutom marknadsföringen och möjligheten för fler att upptäcka företaget när den externa parten är ett större bolag som når ut till betydligt fler.

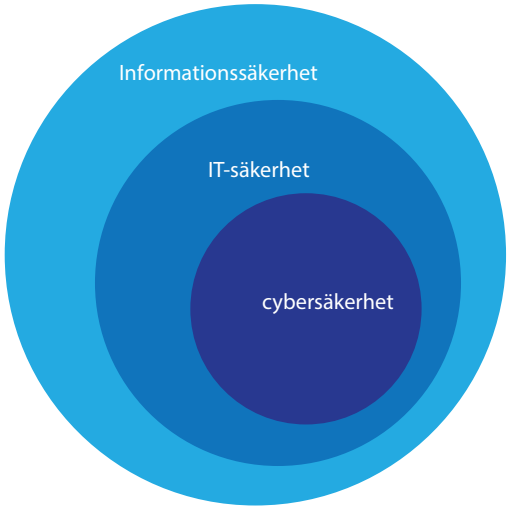
Nätverk är exempel på ett annat digitalt verktyg som kan vara fördelaktigt att ha i verksamheten. Ett nätverk möjliggör effektivare intern kommunikation för organisationen och möjlighet för enheter kopplade till samma nätverk att samverka. Dessutom är ett tillgängligt nätverk något ytterligare att erbjuda besökarna och som resenärer och gäster alltmer förväntar att det finns. Kunderna i besöksnäringen liksom i andra branscher förväntar sig också allt mer att de skall kunna besöka en verksamhets hemsida. Med en hemsida erbjuds resenärer möjligheten att besöka företaget på nätet och få tillgång till information och erbjudanden dygnet runt oavsett var de befinner sig. En hemsida öppnar dessutom upp nya möjligheter för marknadsföring och genom att nå ut digitalt ge betydligt större möjligheter att synas och spridas. En annan fördel för företag att ha en hemsida är att kunna koppla sitt bokningssystem till hemsidan, vilket ger besökare möjlighet att boka utan att behöva kontakta företaget direkt via mejl eller telefon. Företaget kan således hantera bokningarna själva utan direktkontakt med kund i stunden. Detta oavsett om man för in bokningarna manuellt i ett system eller har ett digitalt system kopplat till en extern part via vilken bokningen förs in automatiskt.

Då större delar av verksamheterna i besöksnäringen digitaliseras ökar även behovet av olika enheter i verksamheten. Datorer, mobiltelefoner och surfplattor är enheter som med fördel används för att kunna hantera exempelvis digitala boknings-, kassa- och bokföringssystem, samt för att kunna driva och hantera en hemsida.

Digital säkerhet

Allteftersom en verksamhet blir mer digitaliserad uppkommer en risk för skada på verksamheten från angrepp på verksamhetens IT-miljö. Det finns flera olika angreppssätt på en verksamhet från aktörer med olika incitament för att utföra en attack, där många angrepp kan medföra stora konsekvenser för den drabbade verksamheten. Med ökat hot mot verksamheten ökar behovet av att företagets IT planeras för att skydda organisationens data och de digitala verktyg som används. I och med att det inom besöksnäringen finns ett stort antal mindre verksamheter, vilka därmed har mindre resurser att lägga på såväl digitalisering som på digital säkerhet, kan många verksamheter vara känsliga för angrepp. Samtidigt finns det stora möjligheter med att digitalisera dessa mindre verksamheter vilket öppnar upp för att skapa mer effektiva organisationer, erbjuda ett starkare erbjudande till kunder och ge ökade möjligheter för marknadsföring.

Vad digital säkerhet innebär och hur detta avgränsas är inte helt självklart men det finns ett antal begrepp som definierar olika områden inom fältet. Det mest övergripande är informationssäkerhet, vilket handlar om att skydda information i alla dess former, så väl fysisk som digital information. Ett underområde till informationssäkerhet är IT-säkerhet vilket syftar på att skydda digitala system mot alla typer av intrång och avbrott. I IT-säkerhet ingår alltså att skydda allt som följer av digitalisering. IT-säkerhet kan ses som en samlingsterm för all säkerhet för data i digitala system. Ytterligare en underdelning kan göras vilket då kallas för cybersäkerhet. Cybersäkerhet innebär att skydda nätverk och infrastrukturens tillgänglighet, integritet och konfidentialitet för den information som finns inom cyberodomänen. Konfidentialitet för informationen innebär att den enbart är tillgänglig för de som är behöriga, riktighet innebär att informationen skall vara korrekt och inte skall kunna förändras av någon som inte är behörig medan tillgänglighet betyder att informationen skall vara nåbar då den behöver vara det. Inom ramen för vad som är intressent att undersöka i besöksnäringen kommer vi genom rapporten att undersöka IT-säkerhet enligt följande indelning.



Vad är IT-säkerhet?

Risker för företag i besöksnäringen

Att som organisation vara med om ett cyberangrepp kan ge en rad olika mer eller mindre svåra konsekvenser av olika typer. Det kan dels handla om att en extern part får tillgång till känsliga data från organisationen, dels att organisationen blir hindrad från att komma åt sin egen data eller sina digitala system eller dels att informationen i systemen inte längre är korrekt. Detta enligt tidigare nämnda konfidentialitet, tillgänglighet och integritet. Till exempel kan ett företag i besöksnäringen förlora uppkopplingen till sitt molnbaserade bokningssystem vilket skulle innebära att informationen inte längre är tillgänglig. Någon obehörig skulle kunnat komma åt systemet och ändra i informationen för bokningarna, och skulle därmed ha äventyrat integriteten för informationen som då inte längre stämmer. Det skulle också kunna komma att information som inte skall vara tillgängligt för allmänheten kan kommas åt öppet. Detta hände till exempel för vårdguiden 1177 där miljontals inspelade patientsamtal låg tillgängligt över webben. Personuppgifter kan vara känsliga uppgifter vilka även hanteras i besöksnäringens system och som därmed inte får ligga öppet tillgängliga.

Angriparen kan också ta över system och använda dessa för att utföra olika attacker mot den angripna organisationens kunder eller mot andra organisationer. Att vara möjliggörare för sådana angrepp mot andra system kan göra stor skada på anseende om det verkar som att man inte tagit nödvändiga skyddsåtgärder. Det kan ge dålig publicitet och en negativ inställning till den specifika verksamheten. I en bransch som besöksnäringen där det finns ett stort antal aktörer är det också enkelt som potentiell kund att i många fall välja en konkurrerande verksamhet.

Att tredje part kommer över känsliga uppgifter som kunduppgifter kan leda till att konkurrenskraften för det enskilda bolaget blir lidande, att extra kostnader uppstår eller i värsta fall att lagar bryts. Detta är något som i förlängningen kan leda till böter och andra påföljder för företaget. Sedan 2018 måste alla företag inom EU följa GDPR, vilket är en dataskyddsförordning som tvingar alla organisationer inom EU till att uppfylla krav kring hantering av personuppgifter. [5] Personuppgifter hanteras ofta inom besöksnäringen där bokningar vanligtvis identifieras med personuppgifter, vilka därmed lagras i systemen. Inom GDPR finns sju dataskyddsprinciper som måste följas. I dessa ingår att företag enbart får spara personuppgifter om man efterlever lagar kring datalagring, man får enbart samla in personuppgifter för ett angivet syfte och enbart de uppgifter som krävs för detta syfte. Uppgifterna måste också hållas korrekta och uppdaterade och tas bort då syftet är uppnått. Uppgifterna måste också förvaras säkert så att de inte kan ändras eller stjälas och alla dessa nämnda punkter måste uppfyllas. Dessa punkter är grundprinciperna för GDPR i stora drag men det kan vara svårt att följa den flera hundra sidor långa lagen. Konsekvenserna kan dock bli stora där påföljden för att bryta mot lagen innebär stora bötesbelopp.

Inom ramen för IT-säkerhet ingår den information som finns i de digitala systemen och som följer av digitalisering av verksamheten. Digitaliseringen kan som tidigare nämnt ge ett antal fördelar för organisationen men ju längre digitaliseringen går desto mer beroende blir också organisationen på att de digitala verktygen fungerar. Digitala system kan användas

12:37
•••• 9010
Face ID

och implementeras på olika sätt, vilket ger olika utsatthet för angrepp och tekniska problem. Genom att begränsa vilken information som finns i de digitala systemen kan också den möjliga skadan begränsas men genom att begränsa funktionaliteten i systemen begränsas också värdet som tillförs av systemen. Genom att till exempel inte behandla kunduppgifter eller betalningar digitalt så försvinner risker i och med att datan som lagras inte är lika känslig men effektiviteten i systemet minskar då kunduppgifter antingen behöver sparas analogt och merarbete tillkommer varje gång datan skall kommas åt och olika missförstånd kan uppstå. Men om verksamheten helt förlitar sig på digitala system kan verksamheten få stora svårigheter om något händer med data i systemet eller åtkomst till det. För att minska riskerna kan dubbla system användas eller att en backup hela tiden finns tillgänglig på ett separat system till exempel. Då många företag i besöksnäringen är starkt säsongsberoende och hela årets omsättning ofta skall ske under en mycket kort period kan även kortare avbrott i driften av affärskritiska system kraftigt påverka hela verksamhetens resultat på årsbasis.

Aktörer och incitament

Det finns flera aktörer som kan kopplas till de cyberhot som riktas mot besöksnäringen. Huvudgrupperna av aktörer som utgör hot är kriminella grupper, stater och grupper som är ideologiskt drivna som terrorkopplade nätverk eller hackergrupper [6]. De statliga aktörer som agerar mot eller angriper företag i Sverige har incitament att hämta in information som kan gynna det egna landets statliga intressen eller att dra in pengar till dess ekonomi. De kriminella grupperna har som främsta syfte att tjäna pengar på cyberbrottslighet, medan de övriga grupperna kan ha olika syften utifrån gruppens ståndpunkt. Attacker kan också utföras för att komma åt system som de olika aktörerna sedan kan använda vid attacker mot andra offer. Inom besöksnäringen hanteras ofta personuppgifter i systemen för bland annat bokningar. Personuppgifterna är intressanta för många företag som kan använda de för diverse ändamål som att försöka ge sig på personens konton och inloggningsuppgifter eller för att utföra mer riktade attacker och är därmed värdefulla för någon som vill tjäna pengar på att angripa bolaget utöver att få pengar direkt från bolaget. De kriminella aktörerna kan agera från hela världen mot svenska företag. Desto större pengar det finns att hämta desto större blir också motivationen för de kriminella aktörerna att lägga resurser på att konstruera attacker riktade mot det specifika företaget. Då många företag i besöksnäringen är små med mindre pengar i verksamheten är det troligt att de kriminella utför attacker som har möjlighet att slå bredare snarare än resurstung, riktade attacker mot enskilda företag. Då skyddet mot sådana riktade attacker ofta är mindre hos små bolag som saknar resurser att skydda sig kan dock en riktad attack vara mindre resurskrävande än en motsvarande attack mot ett större offer. Statliga aktörer har ofta stora resurser och kan utföra avancerade angrepp för att landets intressen skall tillgodoses. De länder som kan ägna sig åt sådana angrepp riktade mot Sverige har ofta som mål att hämta information som kan användas för att få ett informationsövertag vid förhandling eller i säkerhetspolitiska frågor gentemot andra länder. Inom besöksnäringen är många aktörer små och behandlar i huvudsak information som inte är användbar av andra länder i sådana frågor och bör därmed inte vara ett prioriterat mål av just denna anledning. De ekonomiska incitamenten för stater består dock där attacker med syfte att dra in pengar till statsapparaten genom olika typer av IT-attacker. Riktade attacker mot mindre företag är mindre motiverade då det finns mindre pengar att hämta här, medan bredare attacker som kräver mindre arbete är mer troliga. Likaså består hotet mot IT-infrastrukturen hos företag i besöksnäringen där de angripande aktörerna sedan kan använda systemen för att utföra nya angrepp. Dessa kan vara riktade mot kunderna till det drabbade bolaget i besöksnäringen vilka kan vara intressanta offer för de statliga aktörerna ur både ett informationsmässigt liksom ekonomiskt perspektiv. Ytterligare en aktör som kan finnas är anställda inom ett bolag som vill angripa bolaget för personliga eller tredje parts räkning. Då en sådan anställd har tillgång till systemet kan denna ofta få stor tillgång till både inställningar liksom data och kan vara mycket skadligt genom att förstöra för verksamheten genom att ändra eller radera data eller hämta ut sådan för att lämna ut till någon annan till exempel.

Sårbarheter

Med digitaliseringen av ett företag följer uppkommer nya sårbarheter med varje nytt system eller digital enhet som introduceras. Enheter som används i verksamheten kan vara datorer, mobiler, nätverk eller olika mjukvaror som alla kan vara en väg in för en angripande aktör. På de enheter som används i verksamheterna finns det ofta ett antal mjukvaror som körs utöver de som används i verksamheten. Till exempel används olika webbläsare, operativsystem samt applikationer. Både de system som används i verksamheten och som finns på och kring enheterna i systemet kommer med sårbarheter. Sårbarheter kan delas in i tre kategorier, brister, funktioner och användarfel [7].

Brister innebär oavsiktlig funktionalitet i systemet som angripare kan utnyttja för att angripa de olika systemen. Dessa brister är ofta vida kända bland aktörer som utför attacker och det finns därmed ett stort antal vanliga attacker som utnyttjar sådan kända brister i olika mjukvaror och system. Denna typ av sårbarhet kan ofta undvika genom att hålla enheter och mjukvaror uppdaterade då sårbarheterna också är kända av de som levererar dessa och därmed kan uppdatera sina system så att bristerna inte längre finns kvar. Dessa kända attacker kan också upptäckas eller blockeras genom att använda IDS (intrusion detection system) eller IPS (intrusion prevention system) som körs på nätverket och letar efter kända attacker i nätverkstrafiken för att kunna informera om att en sådan attack skett eller kunna blockera dessa attacker direkt. En annan typ av brister är så kallade Zero-day-sårbarheter, detta är brister som tidigare, men dessa är ännu inte publikt kända och kan därmed medföra att en angripare som hittar en sådan sårbarhet kommer runt grundläggande skydd. Att hitta dessa sårbarheter är mer resurskrävande och då företagen i besöksnäringen i huvudsak inte hör till de mest värdefulla målen är attacker mindre lönsamma än mot andra aktörer. Däremot kan leverantörerna till besöksnäringen vara tydligare mål för denna typ av attacker där angrepp kan påverka ett stort antal kunder till leverantören. Ett exempel på detta var till exempel då en leverantör till Coop drabbades av en ransomware-attack [8] vilket medförde att Coop inte längre kunde driva sin verksamhet och var tvungen att stänga majoriteten av sina 800 butiker under nästan en vecka med enorma följder för företaget.

Funktioner kan vara sårbarheter för ett system då funktionerna används på ett sätt som de inte är tänkta att användas på. Dessa funktioner och angrepp kan variera i typ och beroende på hur mjukvaror och system är implementerade kan olika funktioner ha mer privilegier eller vidare funktionalitet än vad som är tänkt. Det kan också finnas funktioner som är kraftfulla men som är tänkta att vara begränsade till personer som är auktoriserade men som kan komma att kommas åt även av andra. Detta anknyter till den tredje typen av sårbarhet; användarfel där till exempel en anställd kan komma att ändra i inställningarna i ett system så att sårbarheter öppnas upp eller som lämnar kända standardlösenord. Användare kan stå för många olika risker som t.ex. för svagt lösenord, lämna sin enhet oövervakad men inloggad, råka installera skadlig mjukvara eller bli lurad att dela information från systemet.

Digitala angrepp i besöksnäringen

Det uppstår ständigt nya typer av IT-attacker och så länge det finns incitament att utföra attacker kommer detta antagligen att fortsätta vara ett problem för digitaliserade företag. Dessa attacker utnyttjar på något sätt de sårbarheter som finns, det finns ett antal kategorier av attacker som är de vanligaste typerna av attacker. Inom besöksnäringen är dessa också relevanta men det finns några attacker som utmärker sig genom att de oftare riktas mot verksamheter aktiva i besöksnäringen.

Här följer en lista över de vanligaste typerna av attacker [9] generellt. Ofta kan flera typer av attacker kombineras för att angriparen skall uppnå sina mål.

Vanliga attacker	Beskrivning
Denial of service	Överbelastning av ett systems resurser genom en stor mängd förfrågningar så att systemet inte längre kan svara på riktiga förfrågningar. Detta medför att riktiga anrop som är kopplade till användare eller andra delar av systemet inte längre får något svar.
Man in the middle	En attack där angriparen lyckas få tillgång till trafiken som skickas mellan två parter och kan se vilken information som skickas. Detta kan vara så väl meddelanden som förfrågningar mot system.
Phishing	En angripare skickar mejl som ofta ser ut att komma från en trovärdig avsändare med mål att få tag på känslig information från målet. Angriparen kan skicka länkar som tar offret till en sida vilken lurar offret att ladda ned skadlig kod som malware eller virus alternativt få offret att lämna ifrån sig känslig information. Två underdelningar av phishing är whale-phishing och spear-phishing. Whale-phishing riktar in sina försök mot de viktigaste målen i en organisation då de oftast har mest känslig information och om dessa drabbas av ransomware kan det vara de mest värdefulla. Spear-phishing refererar till mycket riktade attacker där mer resurser läggs på ett mejl till enskilda individer och där mejl ofta ser ut att komma från någon person som offret känner till.
Ransomware	Mjukvara som låser offrets system och håller det gisslan tills det att en lösensumma betalas ut till angriparen. Sådan skadlig mjukvara kan antingen laddas ned från en länk i ett mejl eller från hemsidor.
Lösenord	Lösenord är den vanligaste metoden för användare att verifiera att användaren har åtkomst till ett system. Genom att lista ut lösenordet kan en angripare få mer eller mindre full kontroll över systemet. För att ta reda på lösenordet kan man-in-the-middle-attacker användas, en dator kan användas för att testa en mycket stor mängd lösenord eller så kan en angripare försöka lista ut lösenorden genom att undersöka en individ på sociala medier efter intressen, familj, med mera för att få fler förslag på lösenord att testa.
SQL Injection	Utnyttjar att webbplatser och andra system är beroende av en databas för att lagra och hämta data. Genom att skriva kod för att hämta ut data i olika formulär en användare kommer åt försöker angriparen hämta ut information ur systemet denne inte skall ha tillgång till eller ändra informationen som finns i systemet alternativt försöka stänga ned systemet.
URL-interpretation	En angripare försöker fabricera URL-adresser och använda de för att få tillgång till offrets personliga och professionella data. Detta kan ske genom att försöka komma åt dolda URL:er eller webbadresser för att till exempel komma åt administrationssidor där sedan lösenordsattacker kan användas för att försöka få administrationsrättigheter till systemet.

DNS-spoofing	Angriparen attackerar DNS-servern (domain name system) för offret och skickar trafiken för en viss URL till en alternativ, fejkad, webbplats där offret fyller i information som då angriparen kommer åt.
Sessions-kapning	En typ av man in the middle attack där angriparen tar över en session från offret så att servern tror att angriparen i själva verket är offret och kan därmed få full tillgång till offrets system.
Insiderhot	Attacker som utförs av aktörer inom organisationen och därmed har tillgång till kritiska system med dess inställningar och data. Kan till stor del undvikas genom att enbart ge minsta behörighet som krävs för att de anställda skall kunna utföra sina arbetsuppgifter.
Trojansk häst	Ett skadligt program som är gömt inuti ett program som verkar vara legitimt. Då det legitima programmet startas körs också den skadliga programvaran och kan därigenom få tillgång till systemet.
Drive-by	Skadlig kod bäddas in på en osäker webbplats så när en användare besöker sidan körs den skadliga koden på användarens dator och infekterar denna utan att behöva göra mer än att besöka sidan.
XSS	Cross-site scripting-attacker överför skadliga script genom innehåll som är klickbart som ändras i offrets webbläsare då en webbsida besöks och därmed kan ändra funktionalitet av de klickbara elementen så att de inte längre gör vad offret tror att de gör.
Eavesdrop-ping	Angriparen avlyssnar trafiken på nätverket för att samla in till exempel användar-namn, lösenord eller annan känslig information.
Birthday-attack	Utnyttjar svag kryptering för att identifiera användare och därigenom kan angriparen lyckas kopiera krypteringen och därmed identifiera sig som en användare och därmed få tillgång till systemet.
Malware	Generell benämning av skadlig mjukvara. Malware infekterar offrets dator och ändrar funktionalitet i systemet. Till exempel kan mjukvaran förstöra data, spionera på användarens användning av systemet och nätverkstrafik. Många typer av malware försöker sedan sprida sig vidare till andra datorer som den infekterade datorn är kopplade till. Många av de ovan nämnda attackerna kan också beskrivas som olika typer av malware. Malware kräver att mjukvara instal-leras på systemet och därmed krävs att en användare först gör detta, antingen med eller utan avsikt. Utbildning av de som har tillgång till systemet samt en brandvägg och antivirus som klarar att upptäcka malware.

Utöver dessa attacker som är vanliga i alla branscher finns det ett antal attacker som är mer vanliga i besöksnäringen [10] och som beskrivs i nästkommande tabell:

Vanliga attacker	Beskrivning
Point of sale	Bland de vanligaste attackerna i besöksnäringen där angriparen försöker komma åt kunders kortuppgifter eller betalning genom att angripa själva betalpunkterna som används i verksamheten, som kassasystem, restaurangens kortterminaler, parkeringsautomat eller andra punkter för betalning.
WI-FI nätverks-attacker	t verksamheten eller dess kunder genom att uttnyttja Wi-Fi-nätverket. Till exempel kan ett felaktigt konfigurerat nätverk ge en angripare tillgång till administrationsfunktioner. Angriparen kan också använda egna accesspunkter och försöka få det att se ut som det befintliga nätverket. Genom att kunder och anställda sedan råkar ansluta till angriparens accesspunkt istället för den de tänkt ansluta till kan de därmed få tillgång till den anslutnes system.
Dark Hotel hacking	En typ av phishing-attack där angriparen har reseplaner för ett offer som ofta är högt uppsatta på företag. Genom att angriparen får tillgång till hotellets Wi-Fi laddar de upp skadlig kod till dess server varpå offret får skadlig mjukvara skickad till sig direkt från hotellet som då verkar legitimt och gör det mer troligt att offret att installera det som skickas.

De beskrivna attackerna är enbart en övergripande beskrivning av ett antal vanligare attacktyper. De olika attacker som är underdelningar av dessa attacker utvecklas ständigt och blir mer och mer avancerade. Genom att utveckla nya attacker både inom dessa typer och nya attacker samt kombinationer av attacker uppkommer fler och fler möjliga attacker.

Digital mognad och riskhantering

Hur man som organisation hanterar riskerna som följer av digitaliseringen kan starkt påverka hur starkt skyddet blir av verksamheten jämfört med de resurser som läggs. En digitalt omogen organisation saknar förmåga och medvetenhet om digital säkerhet genom hela organisationen, inklusive ledningen. Dessa typer av verksamheter har ofta också mindre utvecklade digitala verktyg och kan vara mindre beroende av sina digitala system för att driva verksamheten men det finns också de som är starkt beroende av sina digitala system men som inte tagit hänsyn till digital säkerhet. Vidare kan en organisation arbeta med digital säkerhet för att minska riskerna som finns i verksamheten brett och få ett grundläggande skydd mot hot. Att helt säkra organisationen genom att göra alla delar av de digitala verktygen så säkra som möjligt kräver dock mycket resurser. Att göra en analys av verksamhetens

HOTEL

digitala beroende och hur skadliga olika attacker skulle vara kan prioriteringar göras för att vidare minska riskerna för angrepp som är mest skadliga för verksamheten på ett effektivt sätt. Men lika som att en avancerad attack görs som skulle vara mycket skadlig skulle också en attack kunna vara mindre skadlig men å andra sidan vara mer trolig att den sker. Med en analys kan risker rangordnas och fokus kan läggas på organisationens skydd mot de attacker som både är troliga och som skulle ha stor påverkan på verksamheten
En tredje variabel för att analysera hur man skall minska sin risk på ett effektivt vis är att väga in hur mycket resurser som krävs för att minska riskerna från en viss typ av hot. Det finns ofta mycket lågt hängande frukter för organisationer som är mindre digitalt mogna och därmed krävs det relativt lite resurser för att förbättra skyddet avsevärt.

Säkerhetscertifikationer och säkerhetsramverk

För att minska de digitala riskerna i en verksamhet finns det många olika säkerhetsramverk man som organisation kan arbeta enligt. Dessa ramverk syftar att skapa en bästa praxis att följa vid arbete med digitala verktyg. Ett sådant ramverk består av olika riktlinjer och sätt att arbeta för att hantera och minska riskerna. De många olika ramverken man som organisation kan arbeta enligt kan vara mer generella eller mer riktade mot vissa branscher eller typer av organisationer. Ett exempel på ett sådant ramverk som är aktuellt i besöksnäringen är NIST [11] (National Institute of Standards and Technology, USA) cybersäkerhetsramverk som är ett mer generellt sådant. Det grundar sig i att man som organisation först ”identifierar” all utrustning, mjukvara och data som används i organisationen. Därefter ”skydda” dessa enheter, mjukvaror och data samt träna alla som använder enheterna. Den tredje punkten i ramverket är ”upptäcka” vilket syftar till att bevaka system och nätverk för att hitta om obehöriga använder eller skicka data över systemen och därefter undersöka misstänkta fall. Den fjärde punkten i ramverket är ”svara” vilket innebär att ha en plan för hur verksamheten skall handla vid ett upptäckt angrepp. Den sista och femte punkten i ramverket är att ”återställa” efter en attack där data och utrustning återställs och man informerar berörda parter som anställda och kunder om hur man hanterat incidenten. Utöver NIST finns det bland annat ISO 27001 som är en stor internationell standard för IT-säkerhet eller CIS som är ytterligare en. Det finns ett stort antal andra ramverk som, förutom de mer generella, också är mer nischade mot en mindre del av IT-säkerhet eller del av bransch, exempelvis för korttransaktioner.

Ytterligare ett steg företag kan välja att ta är att certifiera verksamheten och genom att följa något standardiserat sätt att arbeta och dessutom få detta konfirmerat via en extern granskning för att få certifikatet. Genom att göra en sådan process kan man som företag visa upp för kunder att man har en stämpel på att företaget arbetar säkert liksom internt också vet att man arbetar på ett säkert sätt.

Digitalisering och IT-säkerhet hos företag i besöksnäringen

Sammanställning av undersökningen

Följande avsnitt presenterar en sammanställning av en undersökning av verksamheter inom besöksnäringen. 32 företag med verksamheter i Östergötland har intervjuats anonymt, och en sammanställning av det insamlade material görs utifrån relevanta områden som framkommit under intervjuerna, som vilka digitala verktyg som används samt vilka risker och hot som finns kopplade till dessa. Vidare sammanställs också företagens syn på digital säkerhet samt utmärkande likheter och skillnader mellan företag av olika storlek med olika typer av verksamheter.

Digitala verktyg och system

Många företag i besöksnäringen är beroende av uthyrning av rum eller utrustning eller något an-

nat som kunden får tillfällig tillgång till och som är begränsat i mängd i verksamheten. Många företag i besöksnäringen har därmed någon form av digitalt bokningssystem för att hantera bokningarna. Systemen kan skilja sig mycket i omfattning, funktionalitet och kostnad där mindre uthyrare exempelvis hanterar bokningar genom systemet mer manuellt genom att de vid bokning får ett mejl skickat till sig, liksom den bokande kunden får ett mail. Många bokningssystem integreras från kundens sida genom att det är integrerat med hemsidan för det säljande företaget i besöksnäringen. Flera av de medelstora företagen inom hotellbranschen, har bokningssystemen anslutna till en eller flera externa parter som Booking.com eller Hotels.com, och besökare kan därmed boka via dessa och där lagda bokningar automatiskt synkas med bokningssystemet. Bland bokningssystemen som används så är de enklaste uppbyggda så att de baseras som en betallösning i grunden och som vid genomförd betalning skickas orderbekräftelse över mejlen till båda de berörda parterna vilket också medför en del manuellt arbete med att gå igenom alla inkomna bokningar. I fler system så finns det ett användargränssnitt för företaget som tar emot bokningarna där de genom gränssnittet, som ofta är webbaserat, kan se och hantera bokningar liksom lägga in bokningar som kommer in via andra kanaler, exempelvis över telefon. I den data som lagras kopplat till bokningarna finns oftast personuppgifter såsom namn, telefonnummer, mejladress och adress till den bokade vilket medför att det är känslig information som regleras av lagar som GDPR och som på något sätt hanteras av bokningssystemen. Ytterligare funktionalitet som kan ingå i bokningssystem, framför allt kopplat till hotell, är att vissa system också kan hantera tillträde till rum och delar av hotellen som kan administreras genom samma system.

De flesta bokningssystem som används i besöksnäringen är på något sätt molnbaserade även om det i begränsat antal fall förekommit lokalt drivna bokningssystem. I de fall där bokningssystemen drivits lokalt har det varit då ägaren haft en tidigare karriär inom IT-sektorn och arbetat med drift av digitala system. När det gäller bokföringssystem används både molnbaserade system och system som körs lokalt i verksamheten, det är ungefär lika vanligt. Vid beslut att skaffa eller byta ut digitala verktyg väljer företag i besöksnäringen i stor utsträckning molnbaserade system. Detta gäller för alla de typer av system som används i verksamheterna.

Samtliga företag som intervjuas för kartläggningen har en egen hemsida för företaget och även nätverk som används i verksamheten. Hur mycket resurser som lagts på att ta fram hemsidan för en verksamhet skiljer sig mycket mellan olika verksamheter. Hemsidorna kan vara mycket simpla och enbart ha en sida med information och mycket simpel eller föråldrad design till att vara mycket avancerade med utarbetad design, ett stort antal vyer och väldigt mycket funktionalitet. Det skiljer också mycket i hur mycket olika integrationer som finns på hemsidorna. Många bolag som har bokningssystem har dock en integration mot detta på sin hemsida så att företagens kunder kan genomföra bokningar och betalningar på deras hemsida.

Hur nätverken som företagen i besöksnäringen använder ser ut skiljer sig också mycket. Det finns allt ifrån företag som använder sitt privata hemnätverk utan några funktioner för gästnätverk där både verksamhetens enheter liksom gästers enheter får ansluta helt utan någon separation och utan lösenordsskydd till de bolag som har avancerade upplägg med ett stort antal accesspunkter, flera virtuella nätverk och funktioner för att där analyser utförs på nätverkstrafiken via IDS eller IPS för att upptäcka intrång. Det vanligaste i branschen med de förutsättningar som finns är dock att företagen har ett nätverk som är någonstans mellan dessa två typer där det finns separata nätverk för verksamheten och gäster som båda är skyddade med lösenord. Anställda på företagen får oftast också vara anslutna till gästnätverket med sina privata enheter. Att det finns nätverk som kunderna kan ansluta till ses ofta som något som tillför värde från verksamheternas kunder. Det finns ett flertal vanliga attacker mot besöksnäringen som koncentrerar sig på nätverket för att komma åt antingen verksam-

hetens enheter eller verksamhetens kunder och det är därmed viktigt att ha ett väl konfigurerat nätverk som inte kan manipuleras enkelt av en angripare och på så vis kompromissa verksamhetens eller dess kunders data eller system.

De kassasystem som används är även dessa ofta molnbaserade, där produkter finns inlagda i systemen men där personuppgifter inte är en del. De genomförda betalningarna kan sedan bindas till de olika bokningarna i systemet. Kassasystemen behandlar generellt kortbetalningar och därmed kortuppgifter som är mycket åtråvärda för potentiella angripare då de om de kommer över dessa uppgifter genom att använda olika upplägg för att få ut pengarna från kopplade konton. Det är på grund av den direkta kopplingen till pengarna som så kallade point-of-sale attacker utförs som ofta riktar sig mot just kassasystem. Kassasystemen som används i besöksnäringen är av lite olika karaktär där den användande verksamheten kan vara olika involverad i implementering och drift av systemet. Antingen kan verksamheten själva vara delaktiga i att implementera systemet genom att själva ha ansvar för att start upp och lägga in produkter och annat som krävs medan andra kassasystem tvingar verksamheten att ta hjälp av en leverantör som implementerar och står för drift och support för systemet.

Risker och hot kopplat till de digitala verktygen i besöksnäringen

Rutiner, policys och riskanalyser

De flesta företag poängterar under intervjuerna att IT-säkerhet är aktuellt och viktigt, men är samtidigt öppna med att det inte är något som de själva har reflekterat särskilt mycket kring eller arbetar aktivt med. Inget av de mindre eller medelstora företagen som intervjuas utbildar sina anställda inom IT-säkerhet eller har några rutiner kring att diskutera digital säkerhet. Få av de mindre företagen har några rutiner när det gäller uppdatering av mjukvaror, system eller digitala verktyg, utan gör systemuppdateringar när de blir tvingade av leverantören att göra det vilket gör att för att fortsätta använda mjukvaran. Detta medför att de leverantörer som inte uppmanar sina kunder att uppdatera mjukvaror eller webbläsare där kända sårbarheter finns blir mer utsatta då det är stor risk för att dessa sårbarheter finns kvar under en lång period under vilken systemet används. Vissa av de större företagen har gjort någon enstaka riskanalys i samråd med leverantör, men även hos de större företagen med en IT-ansvarig har riskanalyser sällan gjorts vilket delvis grundar sig i att det inte finns intresse för att undersöka vilka riskerna är och delvis i att det inte finns kompetens inom bolagen för att veta att det finns risker eller hur de skall analyseras.

Det är få företag i besöksnäringen som har några egna rutiner eller policys alls när det gäller IT- och informationssäkerhet. I många företag är uppfattningen att man inte har tillräckligt med kunskap om vad som skulle kunna göras och borde göras i verksamheten ur en IT-säkerhetssynpunkt. Flertalet företag uttrycker dock att de skulle vilja göra mer för att öka säkerheten och att de skulle vilja öka sina kunskaper och kompetens om digitalisering och säkerhet. Det saknas ofta även backups på data och vid molnbaserade verktyg ser få risker med att det är ett alternativ att data kan äventyras vid till exempel angrepp, misstag eller fel hos leverantören. Bristen på backup kan ge stor påverkan på verksamheterna, framför allt om det sker under den korta högsäsongen. Många organisationer har begränsat med data lagrat lokalt utan den affärskritiska data ligger ofta i tjänsterna i molnet vilket medför att man blir väldigt beroende av sina leverantörer att kunna leverera tjänsten med hög nivå av tillgänglighet och att leverantörerna hanterar data på ett sätt som gör att den går att återställa.

Vanliga typer av IT-attacker är exempelvis phishing och andra länkattacker, vilka framför allt kan komma av att anställda gör misstag eller är

okunniga om att klicka på länkar, oförsiktiga med uppgifter eller liknande. Detta är något företagen är medvetna om och en hel del berättar att detta är något de pratar om inom företaget, även om de inte har någon formell policy för det. Vid en första öppen fråga kring hur man ser på digital säkerhet och hur man jobbar med det svarar majoriteten av företagen att man inte alls arbetar med digital säkerhet, men efter vidare samtal framkommer att de flesta exempelvis använder sig av spamfilter på mejl, har uppdelningar i personalen för vem som har tillgång och behörighet i olika system och att man har separata nätverk för gäster och för verksamheten. Många i verksamheterna tänker alltså på digital säkerhet på någon nivå, men det finns en stor okunskap kring vad som faktiskt är IT-säkerhet. De saker som man tänker på i verksamheterna är oftast på en relativt grundläggande nivå som är enkel att ta till sig och mer omtalad, exempelvis att det är viktigt att ingen utomstående får tillgång till inloggningsuppgifter till viktiga system.

Få företag erbjuder någon typ av utbildning inom digital säkerhet för sina anställda. De flesta företagen i besöksnäringen är mindre verksamheter utan någon IT-avdelning eller någon utbildad IT-ansvarig, och det är därmed svårt för dessa verksamheter att genomföra utbildningar inom IT-säkerhet på arbetsplatsen utan att ta in extern kompetens vilket kostar både pengar och tid då många av de anställda på verksamheterna är säsongsanställda och ofta enbart arbetar några veckor på företaget. Den höga andelen säsongsanställda i verksamheterna medför också att det kommer in många personer i verksamheten och som arbetar med deras system som inte har någon stark koppling till verksamheten och som kan få tillgång till känsliga bitar vilket kan medföra en risk för verksamheterna om behörigheter inte hanteras. Ingen av verksamheterna som undersökts har något ramverk för IT-säkerhet följts, de har inte heller haft något säkerhetscertifikat.

Risker för verksamheterna

De IT-relaterade risker företagen ser för sina verksamheter är att olika digitala system skulle ligga nere under kortare eller längre tid, vilket skulle försvåra arbetet i verksamheten. Detta är något som kan ge stor påverkan på verksamheten på grund av den korta högsäsongen som är utmärkande för företag i besöksnäringen. De flesta företag ser dock inte några större risker för det egna företaget; man ser inte någon anledning till att en angripare skulle vilja ge sig på ett mindre företag i besöksnäringen. Och om man skulle bli angripen, ser man det som en engångshändelse som skulle försvåra arbetet under en kort, begränsad tid. Många företag beskriver att de inte har något känsligt på företaget som skulle vara värt för en angripare att komma åt. Få företag har förståelse för eller kunskap kring vad konsekvenserna skulle kunna bli av ett angrepp och många ser det som osannolikt att ett angrepp skulle ske, och ser i sådant fall främst kortsiktiga konsekvenser. Generellt sett verkar många se situationen mer likt ett inbrott där någon skulle vilja stjäla något specifikt, och tycker då inte att riskerna är särskilt stora då företaget inte hanterar särskilt känsliga uppgifter. Få lyfter det faktum att det kan få konsekvenser att en angripare exempelvis kommer åt företagets besökare och angriper dessa genom företagen. Detta drabbar företaget indirekt då det drabbar deras kunder, och kan få stora konsekvenser på lång sikt, men är inget som lyfts som en risk under någon intervju. Förlorade data som hamnar i fel händer kan ge konsekvenser ur flera perspektiv, både rent juridiskt med lagar som bryts vilket kan ge stora ekonomiska påföljder, och konsekvenser genom dålig publicitet och skadad tillit i kundrelationer. Ett annat perspektiv av konsekvenserna av att en angripare kommer över personuppgifter är att det kan bli rörigt i företagets system med felaktig information, när man inte längre har ett överensstämmande system för vem som har bokat vad och när.

Inloggningsuppgifter och hur de används är något annat företagen i besöksnäringen generellt är medvetna om att de måste vara försiktiga med, men det är samtidigt vanligt att många anställda använder samma inloggningsuppgifter och få har någon direkt policy för informationssäkerhet. Ytterligare en risk är inloggade system som lämnas oövervakade i verksamheten där någon fysiskt kan komma och gå in i redan inloggade

system i verksamheten. Det är något som kan få stora konsekvenser och som är relativt vanligt i verksamheterna, även om företagen själva inte uttrycker att man ser det som en stor risk.

Risker med hemsida, nätverk och behörighet

När det gäller hemsidor finns det många typer av attacker som kan riktas mot hemsidor där företagen i besöksnäringen utsätts för samma hot som i övriga branscher. Då många i de mindre bolagen i besöksnäringen använder sig av egenutvecklade sidor, antingen från grunden eller med wordpress, finns det många som har sårbarheter kopplade till sig. Vilka konsekvenser detta kan få varierar dock också med vilken funktionalitet som finns på hemsidan. De flesta företag ser det som osannolikt att en angripare skulle vilja ta över deras hemsida, och hänvisar återigen till att de inte hanterar några särskilt känsliga uppgifter. Risken med att hemsidan tas över och att kunder riktas till andra ställen som inte är legitima genom lyfts inte fram som en risk från något företag.

Många företag i besöksnäringen har svårt att förklara hur deras nätverk är konfigurerat, detta inkluderar de som satt upp det själva. Nätverksattacker är också vanliga inom besöksnäringen enligt flera källor där man även beskriver att företagets kunder kan vara måltavlor för attackerna.

Generellt används olika behörighetsnivåer i företagen i besöksnäringen, där enbart ett fåtal personer har tillgång till alla funktioner eller alla program. Det är även något som tycks bli allt vanligare, och som många företag är medvetna om.

Förhållande till leverantörer

En risk som en del företag tar upp är att företagets leverantör blir utsatt för en attack, och att data från verksamheten då går förlorat eller att man inte längre får tillgång till systemet. Det är dock inte något som företagen är särskilt oroliga för utan tilliten till de digitala systemen och leverantörerna av dessa är generellt stor. Även de företag som beskriver att deras leverantörer nyligen blivit utsatt för en överbelastningsattack som gjorde att företaget system låg nere i flera timmar, har fortfarande stort förtroende för leverantören och systemen.

Utmärkande likheter och skillnader

Utifrån de olika företagen som kontaktats och vad dessa företag har för egenskaper kan vissa generaliseringar göras. Företagen har olika typer av verksamheter som hotell, restaurang, uthyrning med mera liksom en kombination av dessa. De är också varierande i storlek, både per antal anställda och i storlek på omsättning samt hur pass säsongsbetonade de är. Ytterligare kan vi se att företagen skiljer sig IT-frågor efter vilken typ av person som driver bolagen. Är den ansvariga för drift och beslut också ägare av verksamheten eller är företaget del av en större koncern. Också personliga faktorer, t.ex. ålder hos ägare och beslutsfattare, kan ses som ett attribut av verksamheten.

En tydlig och naturlig skillnad ses mellan stora och små verksamheter där större verksamheter har mer resurser att utveckla sin IT. Detta syns både i hur mycket tid personal har att lägga på IT och i hur mycket pengar som läggs på IT. Det är också naturligt att i mindre bolag med ett fåtal anställda så har den beslutsfattande personen fler ansvarsområden, vilket då ofta inkluderar även IT-frågor. Då företagen blir något större och har fler anställda kan det komma att vara någon annan än just den högst ansvariga i bolaget som är ansvarig för IT-frågor. Vem det är som är ansvarig beror ofta på vem som har haft intresse för området sedan tidigare eller som har mest bakgrundskunskaper. Något som blir tydligt är att de bolag som är större och där den högst upp i hierarkin på företaget är ansvarig för IT-frågor så är dessa frågor oftare högt prioriterade och mer resurser läggs då på företagets IT. Hos de större hotell som medverkat i studien där de antingen ingår i en kedja eller har en extern ägare som inte är operativt ansvarig i verksamheten har det i dessa fall varit hotellchefen som varit ansvarig för IT på hotellet och inte hotelldirektören. De

hotell som tillhör större nationella hotellkedjor har också intern IT-avdelning som de olika hotellen anlitar för sin IT.

Med storlek på verksamheten kan också ses att de minsta företagen, med sina mer begränsade resurser i större utsträckning använder sig av enklare digitala system som de själva till viss del är med att sätta upp. Till exempel använder många av de mindre verksamheterna ett nätverk som de själva satt upp och som då ofta inte är installerade med stark säkerhet. De bokningssystem och kassasystem de använder är också oftare av karaktären att de själva står för att implementera de genom att lägga till produkter med mera än för större bolag. De mindre bolagen gör också i större utsträckning sin egen hemsida än större verksamheter, ofta med någon typ av wordpress-baserade verktyg som kommer med diverse begränsningar liksom säkerhetsrisker om det inte implementeras på ett säkert sätt. Då storleken på företagen ökar outsourcas ofta digitala verktyg och system till en eller flera yttre aktörer. Ofta kommer det först att anlita ett företag som gör en hemsida och denna aktör är sedan också ofta ansvarig för driften av hemsidan. Nästa steg är ofta att också anlita ett företag som är mer ansvarig för IT-infrastruktur. Dessa leverantörer anlitas ofta för att administrera mejl till vilket office 365 har visat sig vara mycket vanligt förekommande bortsett från i de minsta bolagen. I detta paket ingår också molnbaserad lagringstjänst liksom ordbehandling och kalkylark även om det är många verksamheter där dessa inte är kritiska för verksamheten. Leverantörerna av IT-infrastruktur levererar också ofta nätverk till samma bolag. Nätverken som levereras av en sådan leverantör är ofta implementerat med fler säkerhetsfunktioner och av mer kunnig personal och dessa nätverk kan även ha mer avancerade säkerhetsfunktioner, såsom brandväggar som upptäcker intrångsförsök. Samma leverantör kan också ofta komma att leverera kassasystem och kortläsare till verksamheten. Bokningssystemen har de flesta verksamheter själva ansvar för även för de lite större verksamheterna där de själva har direktkontakt med leverantören av dessa. De är även molnbaserade för alla storlekar av företag borträknat ett företag med IT-kunnig personal från tidigare karriär men som även de säger att de kan se fördelarna med ett molnbaserat system och om de hade upphandlat ett nytt system idag hade det troligen varit ett molnbaserat bokningssystem.

Mellan olika verksamhetstyper i besöksnäringen finns det tydliga skillnader i digitaliseringsgrad. Hotell, bed and breakfast, vandrarhem och andra verksamheter som erbjuder boende är generellt mer digitaliserade än vad företag som enbart driver restaurang är. Bland de företag som erbjuder boende har majoriteten av tillfrågade företag, oavsett storlek, någon form av bokningssystem, hemsida samt nätverk som de erbjuder till sina kunder. Företag som främst bedriver restaurangverksamhet har ofta enbart en enklare hemsida utvecklade av bolaget själva eller av en leverantör samt ett enklare kassasystem. Detta gäller även för större bolag med restaurangverksamhet. Det undantag vi sett är en stor kedja med ett stort antal restauranger där ett enklare bokningssystem samt orderläggningssystem finns i verksamheten. Att bolag som restaurangdrivande företag är mindre digitaliserade kan komma från att mer IT i verksamheten inte efterfrågas lika starkt av kunderna till dessa verksamheter och inte tillför samma värde till företagets erbjudande som för till exempel hotell. Det medför också att den digitala risken för dessa verksamheten minskar då de är mindre beroende av digitala system samt att då det inte finns information som angripare vill komma åt i de systemen som finns blir de inte heller ett attraktivt offer. Företag som enbart erbjuder uthyrning av sportutrustning, t.ex cyklar eller kajaker, har generellt svagt digitaliserade verksamheter. Dessa bolag är ofta mycket små och erbjuder sina kunder ett enklare trådlöst nätverk vilket inte säkras upp utan ofta är det privata nätverk som ägaren av bolagen har utan att använda sig av gästnätverk. Dessa bolag erbjuder också ofta någon typ av enklare bokningssystem där känsliga data som personuppgifter kan finnas och som i vissa fall då finns i mindre säkra system eller skickas över mejl.

Hur starkt digitaliserad och hur stark medvetenhet kring IT-säkerhet som finns i de olika

verksamheterna i besöksnäringen kokar ofta ned till hur stor kunskap och intresse som finns hos de individer som arbetar i de olika företagen. Om det finns ett starkt intresse eller kunskap hos ägare eller någon annan ledande i företaget investerar de oftare i mer sofistikerad IT på alla nivåer men anlitar i majoriteten av fallen externa leverantörer av de olika systemen. De företag som är intresserade och har kunskap vet då vad de efterfrågar från leverantörerna och ser nyttan i att investera resurser och pengar i sin IT. Om individerna i företagen i stället är mindre intresserade har de ofta inställningen att de kan lösa mycket själva vilket i många fall medför ett mindre lyckat resultat ur såväl säkerhetssynpunkt liksom vad det tillför för värde till verksamheten. Denna grupp av företag har ofta beslutsfattare som är äldre och som inte är intresserade av IT, varken i sitt liv eller i sin organisation utan ser det mer som något som är nödvändigt än något som kan vara drivande för verksamheten.

IT-leverantörer inom besöksnäringen

På andra sidan av de system och IT-lösningar som verksamheter i besöksnäringen använder sig av finns leverantörerna av systemen. Fem leverantörer som erbjuder bokningssystem och infrastruktur till företag i besöksnäringen där någon person som är insatt i företagets produkt har intervjuats. En leverantör av IT-infrastruktur har också svarat skriftligt på frågor kring hur de och deras kunder arbetar med IT-säkerhet från deras perspektiv. En sammanställning av undersökningen presenteras i följande avsnitt.

Erbjudande

De företag som levererar digitala verktyg och system till besöksnäringen kan delas upp i olika kategorier utifrån vad de erbjuder företagen i besöksnäringen. Det finns det de leverantörer som erbjuder boknings- och kassasystem direkt till sina kunder, men det finns även de som levererar exempelvis kassasystem genom en tredje aktör. Det är då alltså leverantören som erbjuder själva IT-systemet, exempelvis ett kassasystem, medan en tredje aktör säljer systemet till företagen i besöksnäringen. Den tredje parten som säljer systemet till kunden bistår ofta även med att sätta upp, installera och driva systemet åt företaget i besöksnäringen. I de fall där leverantören erbjuder digitala system via en tredje part är det även vanligt att den tredje parten bistår med ytterligare lösningar i den digitala infrastrukturen till kunden. Den tredje aktören står då ofta för att sätta upp och driva exempelvis nätverk, domäner och molntjänster som Office365, inklusive mejl. Det finns också de företag som erbjuder hemsidor till företag i besöksnäringen, dessa kan i vissa fall vara separata och i andra fall vara samma leverantörer som levererar övrig IT-infrastruktur. Det finns därtill även företag som levererar färre delar i infrastrukturen, exempelvis endast nätverk och mejl, utan att leverera kassa- och bokningssystem. I kartläggningen visar det sig att det är vanligt för företag i besöksnäringen att ha samma leverantör för just nätverk och mejl, där företaget står för att sätta upp och driva systemen. När det gäller bokningssystem har undersökningen visat att samtliga intervjuade företag i besöksnäringen har haft direkt kontakt med leverantören utan en tredje part.

Majoriteten av de leverantörer som har intervjuats erbjuder någon typ av bokningssystem till företag i besöksnäringen, och vissa har även hårdvara på plats som är kopplat till bokningssystemet. Vissa av företagen riktar sig mer specifikt mot hotell- och boendeverksamheter, medan de andra levererar system till alla typer av verksamheter i besöksnäringen. Av de företag som intervjuats är tre av leverantörerna större bolag där det hos två är mer uttalat vem det är som har ansvar för säkerheten utan att de har en specifik roll för IT-säkerhet medan det hos det tredje och största är två anställda med rollen IT-säkerhetsansvarig. De två andra leverantörerna som intervjuats är mindre bolag med endast en eller ett par anställda, där dessa personer sköter IT-frågor som en del i sitt dagliga arbete.

Leverantörerna av bokningssystem som intervjuats, både de större och mindre bolagen, erbjuder molnbaserade bokningssystem. Den två största leverantörerna som intervjuats har kunder i flera länder och riktar sig främst till större företag i hotellverksamhet och besöksnäringen. Av de min-

dre företagen som intervjuats har de sitt främsta fokus på bokning av upplevelser, lokaler och uthyrning av sportutrustning. Dessa leverantörer riktar sig framför allt mot mindre företag som själva kan implementera leverantörens tjänst och på så sätt skapa sitt bokningssystem och integrationer mot sin hemsida. Alla leverantörerna av bokningssystem uttrycker att de strävar efter att erbjuda samma tjänster till alla kunder, oavsett storlek och verksamhet, men poängterar att det finns variation i hur stor utsträckning det i själva verket är samma produkt till alla kunder. Detta då många av de större kunderna får mer anpassade lösningar och mer support, vilket bland annat kan fås som ytterligare tjänster. Det företaget som till skillnad från de andra intervjuade levererar IT-infrastruktur, har ett större antal tjänster med allt från IT-support till nätverkslösningar, framför allt riktade mot små och medelstora företag.

IT-säkerhet

Liksom när det gäller företagen i besöksnäringen är det även tydligt hos leverantörerna att ju mindre företaget är, desto mer avgörande är ägarnas intresse för IT-säkerhet. Av de mindre leverantörer som intervjuats med en eller ett par anställda, skiljer sig kompetensen inom IT-säkerhet mycket beroende på personernas personliga intresse. I det företag där ägaren uttrycker ett stort personligt intresse och engagemang för digital säkerhet är säkerhetsfrågor betydligt mer inkluderade i verksamheten än hos den leverantör där intresset inte är lika stort. Hos de större leverantörerna som intervjuats finns det generellt fler tekniskt kunniga personer och system som involverar säkrare funktioner såsom mer kryptering, backup och autentisieringslösningar.

Samtliga leverantörer beskriver att de arbetar med digital säkerhet och att de gör interna riskanalyser, men hon de större bolagen är det tydligare att man arbetar mer aktivt och regelbundet med säkerhetsfrågor exempelvis genom årliga konferenser och regelbundna möten med riskanalyser i fokus. Inget av företagen som intervjuats har idag några säkerhetscertifikat eller följer något cybersäkerhetsramverk officiellt, men de större bolagen poängterar att det är något de arbetar mot och något de planerar att uppnå framöver allteftersom de växer. Inget av de mindre företagen uttrycker att man har någon plan för att uppnå något certifikat eller följa något ramverk officiellt, men tillägger att man arbetar med och diskuterar exempelvis GDPR och andra säkerhetsfrågor. Att ett certifikat inom IT-säkerhet skulle kunna vara en USP (unique selling point) att med locka kunder med är inte något som bekräftas av någon under intervjuerna. För att koppla till undersökningen av företag i besöksnäringen är det inte något som efterfrågas av kunderna, sannolikt i och med den låga kunskapen och kompetensen inom IT-säkerhet. Undantaget är en av de större leverantörerna av bokningssystem som har vissa kunder som är mycket stora och som också ställer stora krav på säkerheten mot leverantören. Således är ett certifikat i nuläget inte att betrakta som en UPS för leverantörerna mot mindre bolag men kan ses som en hygienfaktor för att vara aktuell som leverantör till större kunder. Med en ökad kompetens inom IT-säkerhet i besöksnäringen skulle det kunna bli ett starkare säljargument med ett säkert erbjudande.

Företaget som erbjuder IT-infrastruktur har å andra sidan flera anställda som har certifikationer inom IT-säkerhet och de yttrar sig också om en kultur på bolaget som är starkt influerad av IT-säkerhet med många som har en bakgrund inom IT-verksamheter. De har också i större utsträckning tillgång till kundernas nätverk och system på distans om detta regleras i avtal med kunden, vilket ger dem stor insyn och kontroll över sina kunders system. De arbetar dock tydligt internt med att begränsa denna tillgång för att säkert kunna erbjuda dessa tjänster.

Ett av de större företagen har vissa rutiner kring hur en incident eller en attack skulle hanteras, medan de andra företagen inte säger sig ha några konkreta rutiner utan tar det ifall ett sådant fall skulle uppkomma eller att de arbetar med att ta fram en sådan plan. De leverantörer som gör riskanalyser och har återkommande diskussioner kring digital säkerhet har där även inkluderat

diskussioner kring åtgärder och agerande vid händelse av en attack, även om de förklarar att de saknar några formella riktlinjer eller rutiner att följa vid en sådan situation. Hur en leverantör till företag i besöksnäringen agerar kan påverka hur och i vilken utsträckning kunderna drabbas. Dessutom kan leverantörens egna anseende på marknaden påverkas, sant relationen till och förtroendet hos sina kunder.

Besöksnäringen ur leverantörernas perspektiv

Under samtliga intervjuer poängteras det att kunderna i besöksnäringen har låg kunskap och kompetens inom IT och IT-säkerhet, att den digitala mognaden är låg. Samtliga leverantörer beskriver att de intresse kring säkerhetsfrågor saknas hos deras kunder, och att dessa frågor därför sällan diskuteras med kunder. En IT-ansvarig för ett av de större bolagen uttrycker:

" They don't really care about security, they don't know that much about it"

Just det låga intresset för IT och IT-säkerhet uttrycker samtliga leverantörer är något som generellt utmärker företagen i besöksnäringen, som ofta är små med begränsad kompetens och resurser att lägga på IT. Flera av leverantörerna ser risker med den låga kompetensen hos kunderna; man beskriver de fysiska system som används på plats hos verksamheterna som en risk då de är dåligt uppdaterade och därmed exponerade mot attacker som riktas mot kända säkerhetsbrister i systemen. Leverantörerna beskriver därtill att man ser en annan vanligt förekommande risk då systemen ofta lämnas obevakade men fortfarande inloggade eller att inloggningsuppgifter lämnas på en lapp vid datorn. Detta är en risk då det ger möjlighet för utomstående att komma åt systemen för att hämta och ändra data som finns i systemen. Riskerna kring dåligt uppdaterade system kan till viss del avvärjas då webbläsaren har tillgång till vissa data kring systemen och kan uppmana kunderna att uppdatera dessa innan de tillåts komma åt bokningssystemet. Risken med att systemen lämnas inloggade men obevakade menar man däremot är en betydligt allvarligare risk, då det kräver tydliga rutiner och policys hos verksamheterna själva i kombination med system som loggas ut automatiskt med kort tids inaktivitet.

En av de större leverantörerna, som är det enda företaget med riktigt stora kunder, menar att storleken spelar stor roll för hur mycket krav kunderna ställer; de ser tydligt att ju större deras kunder är desto mer krav ställer de. Detta företag har alltså kunder som är betydligt större än de som kännetecknar besöksnäringen, men poängterar likväl att det även hos dessa, de allra största kunderna, är mycket lågt intresse för och efterfrågan på digital säkerhet.

Flera av leverantörerna erbjuder möjlighet för kunderna att ha varierad behörighet för olika konton i systemen, bortsett de minsta leverantörernas system, för att minska riskerna för och konsekvenserna av incidenter till följd av illvillig eller slarvig personal. Det är svårt att helt och hållet utforma och skydda systemen så att verksamheten inte tar skada av att anställda exempelvis begår ett misstag, men att erbjuda olika behörighetsnivåer samt backup på systemet är en möjlighet att begränsa dessa skador. Alla leverantörer som intervjuats ser detta som en stor risk och således även en viktig säkerhetsåtgärd, och hur behörighetsnivåerna erbjuds och behandlas är något som flera av företagen marknadsför gentemot kunder.

Synen på ansvar

En utmärkande skillnad mellan de större och mindre leverantörerna som intervjuats är att de större leverantörerna tycker sig ha ett betydligt större ansvar för IT-säkerhet än de mindre. De båda mindre företagen förklarar att de inte har något ansvar, men att de trots de har ett intresse av en ökad dialog med sina kunder kring IT-säkerhet. Även de större leverantörerna framför ett tydligt intresse för detta, och menar att detta inte bara skulle gynna kunderna utan även leverantörerna själva. Ett an de större företagen konstaterar:

"Vi är ansvariga om uppgifter skulle läcka ut"

Det är något som står i stark kontrast till vad ett av de mindre företagen uttrycker:

"Nej, vi har inget ansvar, men vi vill gärna ha en dialog och hjälpa till att öka säkerheten för våra kunder - om det är något som skulle efterfrågas"

Samtliga företag återkommer till det bristande intresset från kunders sida när det gäller IT-säkerhet, och ser det som ett hinder mot mer utbredd säkerhet hos företagen i besöksnäringen. Tvåfaktorsautentisiering beskrivs som en av de få säkerhetsrelaterade saker som kunderna efterfrågat, något som kan ha att göra med att det är en konkret sak inom IT-säkerhet som man känner till. Det kan även ha att göra med att andra tjänster man brukar, också använder sig av tvåfaktorsautentisiering. Generellt ser leverantörerna att det enda deras kunder i besöksnäringen känner till kring IT-säkerhet är just tvåfaktorsautentisiering och GDPR, men vad de vidare innebär och hur de bör användas är inget som kunderna tycks ha kunskap kring. En leverantör uttrycker:

"Generellt är GDPR är det enda kunderna har koll på, i övrigt vet många inte alls vad IT-säkerhet handlar om och vad som är viktigt"

En av leverantörerna tar upp att man använder sig av telefonnummer i stället för användarnamn för kunderna som en säkerhetsaspekt. I stället för att logga in på klassiskt vis med användarnamn och lösenord får kunden istället en engångskod skickad till det telefonnummer som är registrerat kopplat till kontot i systemet. Koden gäller under en begränsad tid och kan därefter inte användas för inloggning i systemet, vilket beskrivs som en säkerhetsåtgärd som fungerar bra åt kunderna som annars i många fall skulle slarva med säkerheten på lösenord. Flera av företagen tar upp just risker med att kunder är oförsiktiga med lösenord och har lösenord nedskrivna öppet, exempelvis på en post-it-lapp på datorn, och menar att detta är ett ytterligare tecken på den låga kunskapen kring IT-säkerhet.

Slutsatser

I detta avsnitt följer de slutsatser som dragits efter att ha sammanställt och analyserat resultatet från intervjuerna med företag i besöksnäringen samt leverantörer till dessa.

Digitala verktyg och kompetens

Besöksnäringen kännetecknas av små till medelstora bolag med verksamheter inom livsstil och upplevelser, där verksamheten vanligen är säsongsstyrd med ökad aktivitet under sommarhalvåret. Företagen har därmed vanligen utökad arbetsstyrka med sommararbetare under högsäsong, något som kan ses som en möjlig risk. En säkerhetsrisk för dessa företag är exempelvis att system lämnas olåsta och oövervakade, eller att en anställd begår ett misstag i ett system. Båda dessa risker blir större med en mer oerfaren personal, vilket därmed blir en ökad risk för besöksnäringen som har mycket tillfälliga säsongsarbetare med begränsad erfarenhet och insyn i verksamheten.

En stor del av bolagen i besöksnäringen är familjeföretag, där ägarna ofta arbetar operativt i den dagliga verksamheten. Således finns sällan en specifik roll för IT och IT-säkerhet, utan dessa frågor ansvarar vanligen ägarna för. Verksamheterna är generellt små, och resurser att lägga på säkerhetsfrågor finns inte, resurserna läggs på att digitalisera verksamheterna genom digitala kassasystem, nätverk och hemsidor. De digitala verktyg som används av företag i är typiskt en hemsida, någon typ av nätverk, kassasystem och något bokföringsprogram. För hotell- och boendeverksamheter är det även vanligt med någon typ av bokningssystem. Många av företagen i besöksnäringen har i brist på resurser gjort delar av digitaliseringen själva eller tagit hjälp av en bekant. Många har exempelvis gjort sin hemsida och satt upp sitt nätverk själva, men saknar

kunskap om att driva, underhålla och uppdatera den, och har därmed inte heller kunskap kring säkerhetsaspekter av de digitala verktygen. Det är tydligt att storlek på verksamheten och individuellt intresse hos ägarna starkt påverkar hur väl fungerande och hur tekniskt avancerade verktygen man har är. Således påverkar dessa aspekter även hur sårbara verktygen är och vilken förmåga att säkra dessa man har.

De flesta företag i besöksnäringen är medvetna om sin låga kompetens inom IT-säkerhet, och är dessutom tydliga med att de gärna skulle öka kunskaperna inom verksamheten. Men då både ägare och medarbetare ofta arbetar mycket i den dagliga verksamheten och har ont om tid samtidigt som verksamheterna är små med begränsade resurser, har man inte möjlighet att lägga på att skaffa sig mer kunskap och kompetens. I och med att företagen har begränsad kompetens inom IT och begränsade resurser att lägga på digitala system och säkerhet, har man därtill även begränsad kompetens att veta vad man köper in och vad man kan och bör ställa för krav på leverantörerna. I och med den låga nivån av kompetens inom IT-säkerhet vet man ofta inte vilka sårbarheter som finns i verksamheten. Hos de större företagen med mer resurser har man ofta använt sig av en tredje part som sätter upp leverantörernas system och som driver dessa. Systemen är då generellt mer säkra i och med att en tredje aktör med kompetens inom IT har satt upp systemen och därmed i varierad grad inkluderat säkerhetsaspekter.

Generellt sett ställer få företag i besöksnäringen inte några säkerhetsrelaterade krav på sina leverantörer. Företagen uttrycker att man har stor tillit till leverantörerna, men vet egentligen inte särskilt mycket om hur uppdelningen av ansvar ser ut gentemot leverantörerna. Från leverantörernas syn är det tydligt att storleken på företagen spelar stor roll för hur mycket krav kunderna ställer på säkerheten där större företag ställer fler krav än mindre företag. Enligt leverantörerna är det dock få som ställer krav på, eller har intresse för säkerhetsfrågor. Även hos de allra största kunderna är intresset lågt och kommunikationen med leverantörerna kring IT-säkerhet nästan obefintlig.

Synen på digital säkerhet

Leverantörerna ser inte alltid att de bär fullt ansvar för sina kunders data. De större konstaterar att de tar fullt ansvar, medan de mindre avsäger sig mer ansvar och har det reglerat i sina avtal. Samtliga leverantörer poängterar dock att det ligger i deras intresse att hjälpa sina kunder vid en eventuell attack eller incident, och menar att det skulle gynna såväl leverantörerna som deras kunder att ha en mer öppen dialog kring säkerhetsfrågor. Alla leverantörer är dock överens om att kunskapen och intresset för IT och IT-säkerhet är för låg hos kunderna, och att en dialog kring dessa frågor därför saknas. En fördel för leverantörerna med ökad kunskap och intresse i besöksnäringen är att leverantörerna då skulle kunna använda IT-säkerhet som en USP (unique selling point), vilket man i nuläget inte har möjlighet att göra i brist på efterfrågan.

Många aktörer i besöksnäringen vet inte vad man skulle göra vid en eventuell attack eller incident, man har inga rutiner eller någon plan, de flesta har över huvud taget inte diskuterat frågan.

Få företag i besöksnäringen har någon uttalad policy eller rutiner för digital säkerhet, men är försiktiga med länkar på mejl och har spam-filter samt att många vet att man skall ha lösenord som är säkra även om detta inte alltid efterföljs. Få ser risken att ens företag skulle kunna utsättas för angrepp och ser det ofta som att någon person skulle vilja komma åt något specifikt hos dem och ser inte risker med många attacker som kan vara bredare riktade. Men vet samtidigt att man inte vet så mycket om digital säkerhet och skulle vilja veta mer.

Hot och risker

Det finns många möjliga attacker som kan utföras, både generellt vanliga attacker och attacker som är mer typiskt vanliga för just besöksnäringen. Många attacker kan få allvarliga konse-

kvenser för verksamheten, både på kort och lång sikt. Attacker mot leverantörer kan även de få konsekvenser för företagen i besöksnäringen, för leverantörerna själva samt för relationen och tilliten mellan dessa.

Få företag känner till vilka risker som finns med att använda digitala verktyg och vilka risker som kan drabba dem, majoriteten av företagen menar att det inte ser några risker för den egna verksamheten och kopplar detta till att de inte tycker sig hantera några känsliga uppgifter som kontouppgifter, och därför inte ser något motiv för en attack. Företagen menar därtill att ett angrepp eller incident troligen inte skulle få så märkbara konsekvenser för verksamheten. Det är även här tydligt att kunskapen om IT-säkerhet är låg, och att företagen missar aspekte, som att en attack eller incident skulle kunna drabba deras kunder eller det övriga samhället, vid attacker genom företagen.

De flesta företag är dock väl medvetna av att deras verksamhet är beroende av de digitala verktygen, och även medvetna om att de själva saknar kompetens om risker och hot rörande IT-säkerhet. En risk som leverantörerna ser är att kundernas digitala system lämnas inloggade men obevakade, där illvillig personal eller extern person kan använda systemet utan tillåtelse och därmed kan göra skada. Slarv med inloggningar och inloggningsuppgifter är något som inte ses av aktörerna i besöksnäringen som något de ser som ett säkerhetsproblem utan de ser framför allt potentiella problem med phishing-mail och GDPR. Detta är även något som flera av leverantörerna påpekar, där man menar att det saknas grundläggande kunskaper om vad IT-säkerhet är och vilka risker som finns och som är relevanta.

Framtidsutsikter

För att minska den digitala risken i besöksnäringen skulle kunskap och hjälpmedel behövs. Detta är också något som efterfrågas av både företagen själva och deras leverantörer. Mer kunskap kring de digitala verktyg och system som används, vilka risker finns med dessa och hur man kan skydda sig mot dessa. Leverantörerna upplever brist på intresse kring säkerhetsfrågor från företagen sida, medan företagen själva uttrycker att de har ett intresse mena att de saknar resurser och har för lite kunskap för att kunna avgöra vad man borde prioritera och lägga resurser på inom IT. Det behövs således grundläggande kunskap kring vad digital säkerhet faktiskt är. Många vet redan att det är aktuellt och viktigt och är intresserade, men saknar grundläggande kunskaper om vad det innebär.

Ett enkelt och lättillgängligt sätt för företagen i besöksnäringen att komma åt och få kunskap kring IT-säkerhet är därmed efterfrågat. Det skulle exempelvis kunna vara ett enklare säkerhetsramverk med en introduktion till ämnet och grundläggande information om IT-säkerhet. Dessutom skulle ramverket kunna sätta olika säkerhetsfrågor i relation till olika situationer och verksamheter för att göra det enklare för företagen att förstå vad som är relevant för just deras verksamhet liksom mer konkreta saker man kan arbeta efter för att öka sin digitala säkerhet. Ett ytterligare tillägg skulle kunna vara någon typ av mall att följa vid inköp av digitala system av en leverantör som en enkel lista med de viktigaste sakerna företagen bör tänka på vid inköp av nya system och vad de kan och bör ställa för krav på leverantören.

Litteraturförteckning

[1]
Digitaliseringsrådet, ”Data som strategisk resurs,” Tillväxtverket, Stockholm, 2019.

[2]
Regeringen, ”Strategi för hållbar turism,” Regeringen, Stockholm, 2021.

[3]
Visit Sweden, ”Visit Sweden,” [Online]. Available: https://corporate.visitsweden.com/kunskap/digital-strategi/. [Använd 29 06 2022].

[4]
Region Östergötland, ”Besöksnäringsstrategi Östergötland,” Region Östergötland, 2021.

[5]
european commission, ”europa.eu,” [Online]. Available: https://ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu_en. [Använd 05 07 2022].

[6]
Myndigheten för samhälsskydd och beredskap, ”Cybersäkerhet i Sverige- Rekommenderade säkerhetsårgärder,” 2020. [Online]. Available: https://www.msb.se/contentassets/fe72c449466e4017bd76787762ab9dc5/rapport-cybersakerhet-i-sverige-2020---rekommenderade-sakerhetsatgarder.pdf. [Använd 07 2022].

[7]
National Cyber Security Centre, ”National Cyber Security Centre,” 2015. [Online]. Available: https://www.ncsc.gov.uk/information/understanding-vulnerabilities. [Använd 2022].

[8]
truesec, ”truesec.com,” [Online]. Available: https://www.truesec.com/why-truesec/cases/coop-back-in-business-after-the-largest-ransomware-attack-of-all-time. [Använd 20 08 2022].

[9]
fortinet, ”fortinet.com,” [Online]. Available: https://www.fortinet.com/resources/cyberglossary/types-of-cyber-attacks. [Använd 24 07 2022].

[10]
O. Glib, ”Acropolium,” [Online]. Available: https://acropolium.com/blog/cybersecurity-and-data-breach-threats-in-hospitality-how-to-fix/. [Använd 25 07 2022].

[11]
National Institute of Standards and Technology, ”NIST.gov,” 16 04 2018. [Online].
Available: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf. [Använd 28 07 2022].

BESTÄLLARENS KOMMENTARER

Företag inom besöksnäringen är, som rapporten nämner, typiskt små till medelstora och är ofta starkt säsongsbetonade. Av det följer ett antal utmaningar relaterat till informationssäkerhet som varit kartläggningens fokus. Ett mindre företag kan av uppenbara orsaker inte ha dedikerade roller för samtliga områden, likt ett större företag kan. I stället tvingas personal att vara generalister och hantera sådant som normalt faller utanför egna kompetensområdet. De medelstora företagen kan ha en anställd för ansvar av IT vilket ändå angränsar till IT- & informationssäkerhet och uppvisar vanligen en något högre nivå av säkerhetsmognad än de mindre. De har vanligen en större digital infrastruktur som kräver en sådan roll, därav är även riskexponeringen samtidigt större och ytterligare säkerhetsåtgärder än viktigare. Vidare har de flesta företagen i besöksnäringen en stor variation i beläggning under året vilket löses genom tillfälliga anställningar. Det får implikationer på flera plan. Inte minst blir det svårare att bygga och bibehålla kompetens inom företaget även om intresset och viljan finns. Här finns ett behov av enkla och kostnadseffektiva åtgärder för att höja den totala nivån av säkerhet. Det kan exempelvis innefatta att aktivera tvåfaktors-autentisering på mailen och en översyn av lösenorden så att de är tillräckligt starka och unika för olika verksamhetskritiska konton.

Ett inte helt ovanligt resonemang från mindre företag att är att de inte sitter på information som har något direkt värde för en illasinnad aktör. Här bör dock understrykas att antagonister har olika fokus och metoder för att nå sina mål. Vissa grupper riktar sina fulla resurser mot enskilda ekonomiskt starka bolag för möjlighet till stor avkastning medan andra grupper och individer kan fokusera på en bredare grupp av enklare måltavlor där kvantiteten ändå gör det lukrativt. Ett s.k. ransomware kan exempelvis ”kidnappa” filerna som finns tillgängliga i systemen och orsaka att alla digitala verktyg förblir otillgängliga till dess att en lösensumma betalas. Lösensumma är inte heller någon garanti för att filerna sen låses upp som utlovat. Andra konsekvenser behöver inte föregås av en incident. Företag som felaktigt hanterar personuppgifter kan göra sig skyldiga till lagbrott och resultera i kännbara böter för en redan resursbegränsad verksamhet. Det kan därmed konstateras att det finns många skäl att se över säkerhetsbilden även för de företag som anser sig inte hantera någon viktig information. Ambitionen bör vara att höja sig en nivå för att inte vara en av de mest attraktiva och utsatta måltavlorna.

Riskmedvetenheten hos bolagen är i princip obefintlig kopplad till ovanstående resonemang kring att man inte upplever att man har någon information som är intressant för en illasinnad aktör. Detta innebär ofta att man underlåter enkla åtgärder som att säkerhetskopiera filer och ta backup på kritisk information. Verksamheterna har inte heller reflekterat över vad som, i deras kontext, är att beakta som kritisk information. De mindre resursstarka har typiskt också fått hjälp av en IT-kunnig bekant för att sätta upp hemsida, nätverk etc vid ett enstaka tillfälle utan vidare tanke på kontinuerligt underhåll som uppdateringar, lösenordshantering etc. Här är det vår bedömning att även enkla insatser kan ha stor och avgörande betydelse för verksamhetens kontinuitet. Att till exempel informera och utbilda i enklare riskanalys och säkra rutiner, uppdateringar och backup skulle förmodligen

höja bolagens resiliens avsevärt till en relativt liten ansträngning.

Det blir i intervjuerna också tydligt att inköp av tjänster och system till huvuddelen fokuserar på funktion och inget eller lite rörande datasäkerhet. Vid direkta frågor utgår verksamheterna ofta ifrån att deras leverantörer har koll på den biten och reflekterar inte mycket över eget ansvar i frågan. Vid samtal med leverantörer framgår det ibland att de utgår ifrån att verksamheterna har koll på och gör backup av sin data. Det finns alltså en diskrepans här i vart ansvaret ligger. Bedömningen här blir att det, med relativt enkla medel, bör gå att guida verksamheterna i sin kravställning gentemot sina leverantörer vad gäller vart ansvaret ligger i olika frågeställningar som t.ex. dataansvar, backup och rutiner för återställning vid behov. Ofta är det leverantörer som är främsta måltavlan vid molnbaserade cyberintrång. Därav är det kritiskt att de har gjort ett gediget säkerhetsarbete och fortsätter arbeta aktivt med säkerheten såväl i egen infrastruktur som i de produkter och tjänster som erbjuds mot kund.

För att brygga utmaningarna och höja lägstanivån för informationssäkerheten i besöksnäringen behövs olika former av stöd för företagarna. Det kan handla om utbildningsinsatser där man på ett pedagogiskt vis förklarar de ofta relativt enkla åtgärder som kan vidtas för att minska företagets risker. Andra insatser kan vara att genomföra workshops för relevanta scenarier kring den egna verksamheten. För de som har möjlighet är riktade stöd från branschexperter även något som bör ge en god effekt på säkerheten. Genom att på olika vis så frön till tankar och diskussioner och att utforska sätt att höja företagens awareness så kan vi höja vår lägstanivå av resiliens mot cyberangrepp. Ett ytterligare viktigt inslag är att vi gemensamt sprider våra kunskaper och erfarenheter till varandra och lära oss var vi hittar goda källor till information. På så vis kan vi även bidra till att höja hela samhällets lägsta nivå. Detta i en tid då det är mer viktigt än någonsin att stå enade för ett starkt och sammansvetsat Sverige.

Det offentligt finansierade innovationsstödsystemet spelar här en central roll. Besöksnäringen är en bransch där det satsas en hel del riktade insatser för att stärka dess förmåga att ställa och nyttja digitala teknologiers möjligheter. Pengarna kanaliseras ut genom myndigheter som Tillväxtverket och Vinnova för att finansiera verksamheter och projekt hos olika företagsfrämjande organisationer och projekt. Vi tycker det åligger ett stort ansvar på de aktörer som bidrar och stöttar besöksnäringens digitala omställning att aktivt lyfta frågan om säker digitalisering. Att erbjuda stöd inom affärsutveckling är idag ytterst komplext vilket gör att det krävs nya samverkanstrukturer och roller för att lyckas med detta. Vi tror att lösningen finns i att utgå från den infrastruktur som man redan investerat i, till exempel Science Parks för att ge dem uppdrag att fungera som kunskapsnoder och intermediärer. Uppgiften blir sedan att genom samarbeten med aktörer som Almi, Regionala utvecklingsenheter, kluster och Destinationsbolag säkerställa att man bidrar till att höja den generella kunskapsnivån inom området och integrerar frågan i företagets existerande affärsplanering. Denna pilot är ett lysande exempel på hur två offentliga aktörer samverkar med marknaden för att nå nå ut. För att det ska ge en långsiktig effekt är det viktigt att vi baserat på de lärdomar som görs satsar på att växla över det från en pilot till en mer långsiktig satsning.