Omslagsbild: Julia Kivelä
Lilla bilden på omslaget: Tero Takatalo-Eskola

10 PUNKTER FÖR ATT FÖRBÄTTRA CYBERSÄKERHETEN I RESEBRANSCHEN

ANM: Utvecklingsprojekt som främjar turistnäringens återhämtning 2020–2021. Turismens ansvarsfullhet synlig i Mellersta Finland

VISIT Jyväskylä REGION

jamk

10 punkter för att förbättra cybersäkerheten i resebranschen

01 Identifiera och gör en lista på information som är kritisk med tanke på företages verksamhet

Med tanke på företagets verksamhet och dess fortbestånd är inte all information lika kritisk.

Kritisk information identifieras av att företagets verksamhet allvarligt äventyras om informationen inte är tillgänglig, dess innehåll förvanskas eller blir offentlig. Även affärsplaner, planer och offerter gällande beställningar som förbereds samt uppgifter i register för fastighetsautomatik eller anordningsservice kan vara kritisk information för företaget.

Särdrag i resebranschen är att mycket uppgifter gällande person- och betalkort behandlas. Behandlingen av dessa uppgifter bör ägnas särskild uppmärksamhet.

02 Kartlägg företagets digitala verksamhetsmiljö och gör en lista på system som hör dit

Företagets digitala verksamhetsmiljö består av de enheter där företagets information behandlas, överförs eller sparas. Dessa är till exempel datorer, adaptrar, skrivare, mobiltelefoner, kassa-, försäljnings, beställnings- och e-postsystem. Även video-, passage- och fastighetskontroll- samt låssystem är bra att beakta.

Den digitala verksamhetsmiljön det vill säga använda enheter, applikationer och system ändras ständigt i den snabba resebranschen. Nya enheter kan också komma mitt under en verksamhetsperiod, varför en regelbunden uppdatering av listning är att rekommendera.

03 Försäkra dig om att säkerhetskopieringen av uppgifterna är ändamålsenligt gjord

Se till att information som är kritisk och viktig med tanke på verksamheten säkerhetskopieras och att kopiorna förvaras på ett säkert ställe. Ta hänsyn till alla enheter där information behandlas, till exempel datorer, surfplattor och mobiltelefoner. Säkerhetskopiorna ska skyddas mot utpressningsprogram och otillåten användning. Det är också bra att emellanåt öva på återhämtning av säkerhetskopieringen.

Det lönar sig att bestämma rytmen i när säkerhetskopiering enligt för hur lång tid affärsverksamheten påverkas av att informationen försvinner och beakta säsongerna i den egna turismverksamheten.

04 Installera antispionapplikation för sabotageprogram i de enheter som används och gör programuppdateringar

Det enklaste tekniska sättet att skydda informationen är att hålla antispionapplikationerna för programvara och sabotageprogram uppdaterade. I alla enheter som har tillträde till företagets informationssystem borde antispionapplikation för sabotageprogram installeras. Det är viktigt att regelbundet uppdatera operativsystemet och programvaran i enheterna, även i adaptrarna.

Det lönar sig att göra installationerna i programvarorna och deras uppdateringar bara med program erhållna från tillförlitliga källor.

05 Ta reda på ansvar och förpliktelser gällande cybersäkerhet och dataskydd för de externa tjänsterna som företaget använder

Serviceleverantörens ansvar och förpliktelser är bra att utreda till exempel vad som gäller att skydda, spara eller anmäla avvikelser. Något som bör beaktas är också tillgången till information eller eventuell överföring till följande serviceproducent vid avtalets slut. Dessa saker är ofta lättast att utreda redan i anskaffningsskedet. För de kritiska uppgifternas och systemens del såsom internetanslutning lönar det sig att i serviceavtalet precisera konkreta krav för deras användbarhet. Det lönar sig också att utreda vilka förpliktelser avtalen eventuellt ställer på beställaren.

För turistnäringen är det typiskt att samarbete görs med olika leverantörer av försäljnings- och marknadsföringsplattformar. Det är värt att samarbeta och det ökar ofta betydligt försäljningsvolymen. I samband med att samarbetet påbörjas är det ändå ansvarsfullt att kontrollera ansvar och förpliktelser gällande data- och cybersäkerheten.

06 Upprätta instruktioner för dataintrång eller dataskyddsbrott

När man är förberedd på dataintrång eller cyberavvikelser påskyndas åtgången till normalsituation. Saker som ska planeras är till exempel följande: vem ber man om hjälp för att utreda situationen samt hur och vad informeras personalen, kunderna och eventuella samarbetspartner om det som skett. Nödvändiga åtgärder kan dessutom också vara myndighetsanmälningar till polisen, Cybersäkerhetscentret och eventuellt till dataombudsmannen. Det är bra att på förhand upprätta en kriskommunikationsplan som innehåller ett färdigt meddelandeunderlag.

I resebranschen är ansvarsfullt agerande, kundernas integritet och säkerhet särskilt betydelsefulla – även för att avvärja ryktesskador. Förberedelser på förhand minimerar eventuella skador av störningar.

07 Ta starka lösenord i bruk och använd inte standardlösenord

Svaga lösenord och standardlösenord är en verklig cybersäkerhetsrisk. Standardlösenord ska bytas i samband med ibruktagande av enheter till exempel till en mening som är lätt att minnas. Användarnamnen ska vara personliga, och onödiga användarnamn ska tas ur bruk. Lösenord ska sparas säkert, men ändå på så vis att de alltid finns tillgängliga till på förhand överenskomna personer. Om det finns mycket lösenord, ökar användningen av ett hanteringsprogram för lösenord säkerheten och det spar tid.

Säsongsarbete och de säsongsanställda det för med sig är mycket typiskt för turistnäringen, och därför bör särskild uppmärksamhet fästas vid lösenordspraxisen. Det lönar sig i princip att begränsa behörigheten till ett minimum i synnerhet för säsongspersonal och praktikanter och för övriga delar följa ovan nämnda allmänna anvisningar.

08 Var beredd på att mobilenheterna kan bli stulna eller försvinna

Via en försvunnen enhet kan man få tillgång till företagets konfidentiella uppgifter eller med hjälp av dessa genomföra åtgärder som antingen avsiktligen eller av misstag orsakar skada. Det lönar sig att låsa användargränssnittet för enheterna när det inte finns personal på arbetsplatsen. Det lönar sig att på förhand instruera om och öva på att lokalisera, låsa, logga ut från konton och tömma mobilenheter som är utsatta för stöld.

Ofta är den förlorade informationen mer värdefull än själva den fysiska enheten.

09 Ge en person i företaget ansvar att sköta företagets informations- och cybersäkerhet

Ansvarspersonens uppgifter är bland annat introduktion och handledning för personalen och att försäkra sig om att informations- och cybersäkerheten har beaktats i företagets riskkartläggning och serviceavtal. I uppgiften kan man vid behov få hjälp av en extern serviceleverantör.

I ett turistföretag är det bättre att hellre ge uppgiften till den ordinarie personalen än till en säsongsanställd eller skapa partnerskap om köptjänst för en längre period. Det är ändå bra att observera att företaget inte kan utkontraktera själva ansvaret och att varje anställd, även säsongsbiträden, för sin del sköter informations- och cybersäkerheten.

10 Upprätta företagets riskkartläggning och en skriftlig riskhanteringsplan

I centrum av riskkartläggningen, där även cybersäkerheten är beaktad, lönar det sig att lyfta fram företagets kritiska information och funktioner samt att granska sannolikheten och effekten av de händelser som hotar dessa.

Utifrån kartläggningen kan åtgärderna riktas till att få ordning på de viktigaste punkterna.

Upprätta årsklocka som cybersäkerhetsåtgärd

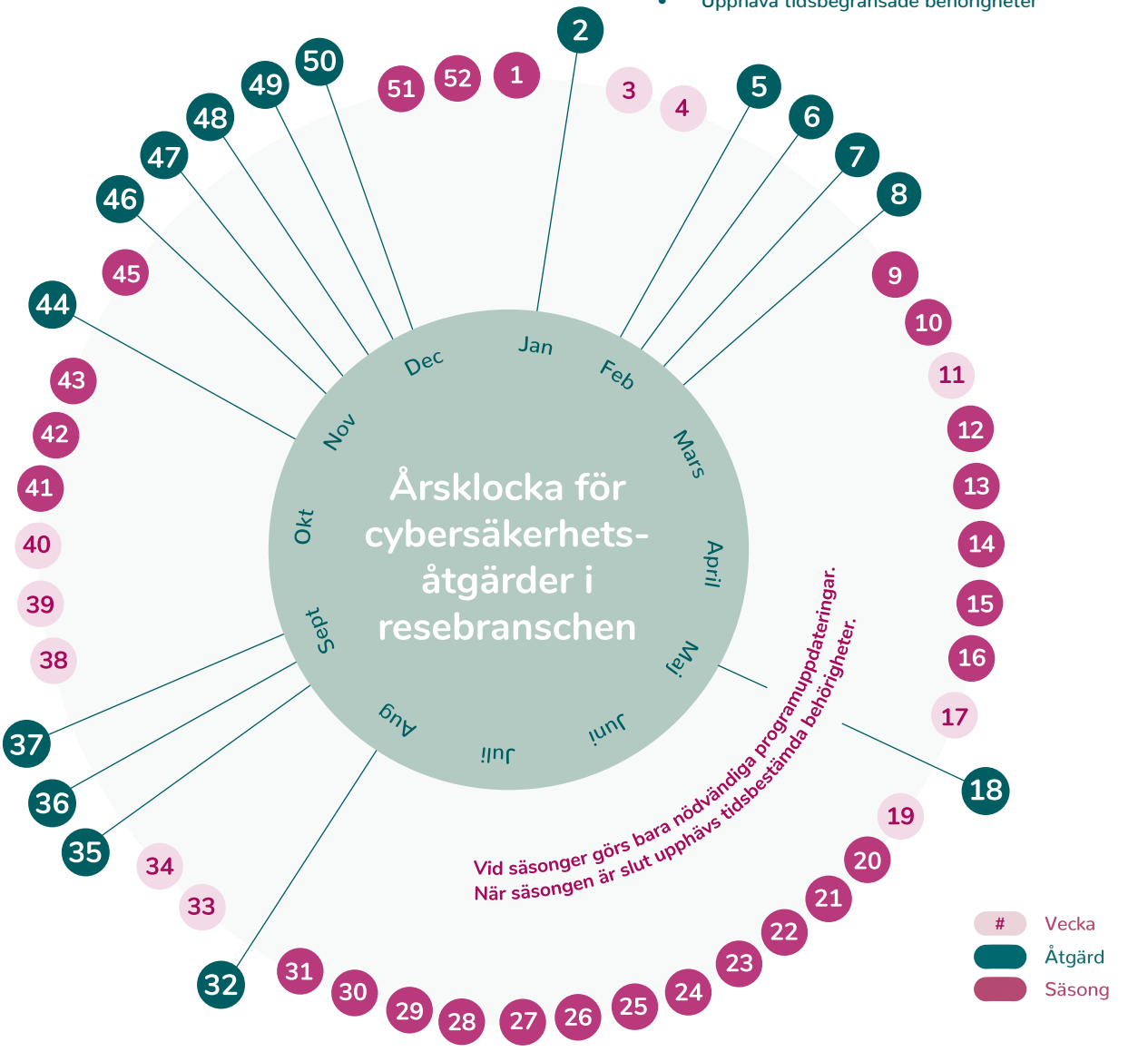
Varje företag har sin egen typiska årsrytm där takten bestäms av säsongsperioderna i turismen. En betydande del av åtgärderna inom cybersäkerheten kan göras utanför turismsäsongen och det lönar sig också. För att upprätta en årsklocka lönar det sig först att upprätta en åtgärdslista som man försökt göra i logisk och kronologisk ordning.

När listan är upprättad kan åtgärderna delas under kalenderåret i regel utanför säsong. Det lönar sig ändå att observera att en del av åtgärderna kan vara kontinuerliga, även under säsongsperiod. En del av åtgärderna kan upprepas flera gånger under året, till exempel att ta bort behörigheten för säsongsbiträden efter säsongen eller att byta lösenord.

I följande exempel finns tre säsongsperioder beskrivna med röd färg. Med grön färg har skydds- och beredskapsåtgärder beskrivits som planerade utanför säsong.

Exempel på åtgärdslista:

- Definiera kritisk information
- Kartlägga digital verksamhetsmiljö
- Kontrollera behörigheterna
- Upprätta riskkartläggning
- Upprätta hanteringsplaner för risker
- Kontrollera de gällande serviceavtalens aktualitet
- Göra programuppdateringar
- Byta lösenord
- Upprätta/uppdatera verksamhets- och informationsplaner för dataskydds- och cyberavvikelser
- Verkställa hanteringsplan för risker
- Bekräfta att säkerhetskopiering lyckats
- Kontrollera antivirusskyddets omfattning
- Uppdatera introduktionsmaterial gällande dataskydd och cybersäkerhet
- Upphäva tidsbegränsade behörigheter



Vecka Åtgärd

2 Byta lösenord
5 Säkerställa att säkerhetskopieringen har lyckats
6 Kontrollera antivirusprogrammets omfattning
7 Uppdatera introduktionsmaterialet gällande dataskydd och cybersäkerhet
8 Verkställa hanteringsplan för risker
18 Byta lösenord
32 Byta lösenord
35 Kartlägga den digitala verksamhetsmiljön
36 Kontrollera behörigheterna
37 Definiera kritisk information
44 Byta lösenord
46 Göra riskkartläggning
47 Upprätta hanteringsplan för risker
48 Kontrollera aktualiteten i de serviceavtal som är i kraft
49 Göra programuppdateringar
50 Upprätta/uppdatera verksamhets- och informationsplaner för dataskydds- och cyberavvikelser