Module 10: Cyberbeveiliging en cyberweerbaarheid in toeristische Mkb's

DIGITOUR

Co-funded by the
Erasmus+ Programme
of the European Union

Project titel: Building Digitalisation Readiness in the Tourism SME sector.

Projectacroniem: DIGITOUR

Projectnummer: 2021-2-IE01-KA220-VET-000048348

Module: Cyberbeveiliging en cyberweerbaarheid

Primaire doelgroep: Mkb's in de toeristische sector

Secundaire doelgroepen: Deskundige aanbieders van beroepsonderwijs en -opleiding, vertegenwoordigers van het toerisme en in-company trainers.

Geschatte tijd: 120 tot 150 Minuten

Doelstellingen: De doelstellingen van deze module zijn om:

- Deelnemers inzicht te geven in de uitdagingen, risico's en het belang voor cyberbeveiligingssystemen.
- Vertrouwd te raken met de basisconcepten en technische termen cyberbeveiliging en cyberweerbaarheid;
- Deelnemers te laten kijken naar de toekomst van de toeristenindustrie met ontwikkelde vaardigheden op het gebied van cyberbeveiliging en cyberweerbaarheid.

Leerresultaten: Na afronding van deze module ben je in staat om:

- De betekenis van de termen "cyberbeveiliging" en "cyberweerbaarheid" beschrijven en begrijpen hoe deze essentieel zijn voor elk type toeristische aanbieder;
- Aan te tonen dat je de basisprincipes en essenties van cyberbeveiliging en cyberweerbaarheid begrijpt;
- De belangrijkste cyberrisico's en aanvallen van de toeristische sector te begrijpen.
- De belangrijkste punten van effectieve, veilige en weerbare cybersystemen te bespreken en herken je de belangrijkste normen voor cyberbeveiliging en cyberweerbaarheid.

Inhoudsopgave

10.1 Inleiding: leidende principes en definities....4
10.2 Cyberbeveiliging en cyberweerbaarheid in context 7
10.3 Cyberkwetsbaarheid van toeristische mkb's....13
10.4 Cyberdreigingen in het mkb in het toerisme....15
10.5 Goede cyberpraktijken voor mkb-toeristen....17
10.6 Conclusie....23
10.7 Lezen en aanvullend materiaal....24

Dit project is gefinancierd met de steun van de Europese Commissie. De verantwoordelijkheid voor deze publicatie ligt uitsluitend bij de auteur; de Commissie kan niet aansprakelijk worden gesteld voor het gebruik van de informatie die erin is vervat

Co-funded by the Erasmus+ Programme of the European Union

10.1 Inleiding: leidende principes en definities

Wat is cyberbeveiliging?

Definities van cyberbeveiliging variëren, maar over het algemeen verwijzen ze allemaal naar de veiligheid van cyberspace.

Cyberspace is de dynamische en virtuele ruimte die verschillende computersystemen met elkaar verbindt.

https://northafricapost.com/42416-morocco-is-not-a-cyber-jungle-defense-administration-tells-amnesty.html

Cybersecurity bestaat uit **2 sleutelbegrippen:**

1. Cyber heeft betrekking op de technologie die systemen, netwerken en/of data bevat.
2. Beveiliging heeft betrekking op de bescherming die systeembeveiliging, netwerkbeveiliging en applicatie- en informatiebeveiliging omvat.

De EU definieert cyberbeveiliging als "de activiteiten die nodig zijn om netwerk- en informatiesystemen, de gebruikers van dergelijke systemen en andere personen die door cyberdreigingen worden getroffen, te beschermen".

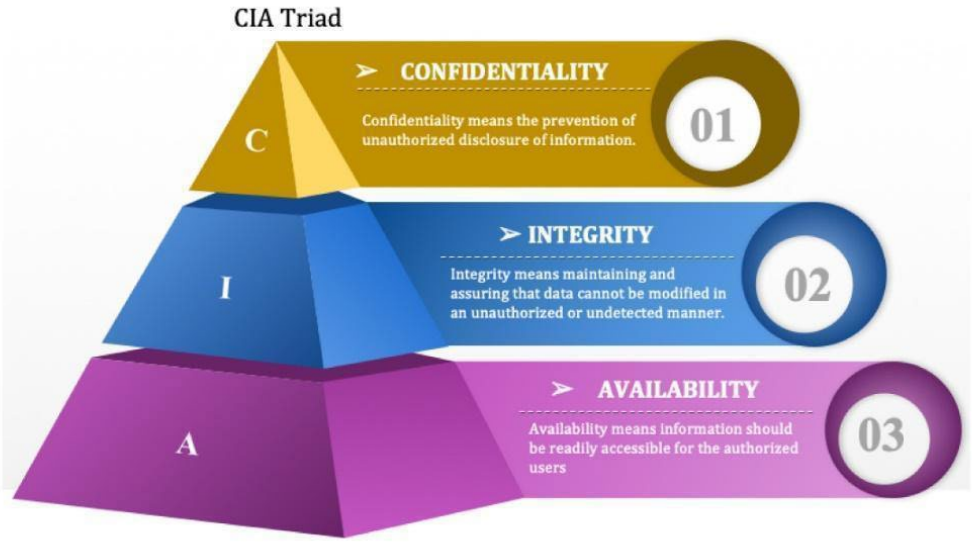
Vertrouwelijkheid, integriteit en beschikbaarheid staan bekend als de 3 belangrijkste principes van cyberbeveiliging:

- ***Vertrouwelijkheid:*** vertrouwelijkheidsmaatregelen voorkomen dat gevoelige informatie wordt vrijgegeven aan onbevoegden (bijv. gegevensversleuteling, tweefactorauthenticatie).
- ***Integriteit:*** integriteitsmaatregelen handhaven de consistentie, nauwkeurigheid en betrouwbaarheid van gegevens gedurende de gehele levenscyclus door te voorkomen dat gegevens worden gewijzigd door

onbevoegde partijen (bijv. back-ups van gegevens, gebruik van bestandsrechten).

- ***Beschikbaarheid:*** beschikbaarheidsmaatregelen zorgen ervoor dat informatie consistent en gemakkelijk toegankelijk is voor de betrokken geautoriseerde partijen en onderhouden de hardware- en softwaresystemen die die informatie bevatten en weergeven.

Over het algemeen verwijst cyberbeveiliging naar elk aspect van het



beschermen van een organisatie en haar werknemers en haar bedrijfsmiddelen tegen cyberdreigingen of -aanvallen.

https://thingscouplesdo.com/what-is-cia-triad-and-how-does-it-work/

Wat is cyberweerbaarheid?

In de bedrijfswereld biedt cyberweerbaarheid een meer holistische manier voor digitale bedrijfscontinuïteit. Het is een nieuw concept, digitale fitness genoemd.

De EU definieert cyberweerbaarheid als *"het vermogen om elektronische gegevens en systemen te beschermen tegen cyberaanvallen, en om de bedrijfsvoering snel te hervatten in geval van een succesvolle aanval".*

In de geavanceerde dreigingsomgeving falen traditionele beveiligingstactieken gericht op cyberbeveiliging. Geen enkele organisatie kan tegelijkertijd

wijzigingen doorzoeken, kwetsbaarheden volgen, beveiligingsbeleid toepassen op verschillende systemen.

Om deze concurrerende uitdagingen het hoofd te bieden, moeten organisaties hun beveiligingshouding veranderen van een defensieve houding gericht op malware naar een meer realistische en weerbare benadering - een cyberweerbaarheidsbenadering (Symantec, 20 14).

Het concept van cyberweerbaarheid kan worden beschouwd als een raamwerk met 5 hoofdpunten:

1. **Voorbereiden/identificeren:** de beveiliging van het bedrijf begrijpen en potentiële risicoposities identificeren om beveiligingsproblemen aan te pakken;
2. **Beschermen:** inzicht in het bedreigingslandschap van het bedrijf (bijv. het niveau van kwetsbaarheid en risicotolerantie) zorgt voor een beschermende infrastructuur;
3. **Detecteren:** zodra er beschermende maatregelen zijn getroffen, kunnen passende activiteiten worden opgezet om snel een aanval te detecteren, getroffen systemen te beoordelen en een tijdige reactie te garanderen;
4. **Reageren:** deze fase is van cruciaal belang om richtlijnen te geven over welke activiteiten kunnen helpen de reactietijd te verkorten en de impact van een aanval te beheersen zodra deze wordt gedetecteerd;
5. **Herstel:** het ontwikkelen en implementeren van de juiste systemen voor gegevensherstel in het geval van een cyberaanval, wat een essentieel onderdeel is van elke weerbare beveiligingsstrategie.

https://w ww.amdhservicesltd.com/how-to-build-a-cyber-resilient-infrastructure

Hoe zijn cybersecurity en cyberweerbaarheid met elkaar verbonden?

Cyberbeveiliging en cyberweerbaarheid lijken vaak onderling uitwisselbaar omdat ze beide betrekking hebben op cyberveiligheid, maar ze zijn niet hetzelfde:

- Terwijl cyberbeveiliging verwijst naar een organisatie die haar bedreigingen beperkt door zich te concentreren op proactieve houdingen tegen de groeiende verspreiding van cyberaanvallen;

- Cyberweerbaarheid daarentegen verwijst naar een organisatie die de potentiële schade en de bijbehorende verliezen zoveel mogelijk beperkt zodra er al een aanval heeft plaatsgevonden, terwijl de normale gang van zaken wordt hervat.

10.2 Cyberbeveiliging en cyberweerbaarheid in context

Cyberbeveiliging en cyberweerbaarheid in het toerisme

In de context van toerisme en reizen is digitalisering een sterke factor geworden voor het bedrijfsleven in de digitale wereld van vandaag.

Cybersecurity en cyberweerbaarheid zijn belangrijk als digitale innovatie die ze waarborgen:

- Digitale innovatie herdefinieerde de toeristische ervaring en heeft geleid tot een verhoogde gevoeligheid van het toerisme voor veiligheidsrisico's.
- Cybersecurity en cyberweerbaarheid zijn instrumenten die de sector vormgeven en zorgen voor een veiligere toekomst voor de mkb-sector toerisme en reizen.

Technologie speelt nu een integrale rol in bijna elk aspect van de reis- en toerisme-ervaring:

- Van het inspireren van toeristen tijdens de koopfase van de consumentenreis,
- Tot het achterlaten van online beoordelingen in de fase na aankoop.

Hierbij gaat het vaak om online transacties, klantgevoelige informatie, cloudintegratie en digitale betalingstechnologie, waardoor de digitale voetafdruk van toeristische bedrijven is toegenomen, waardoor ze zijn blootgesteld aan cyberdreigingen en -aanvallen, waarvan sommige cybercriminaliteit kunnen vormen (Paraskevas, 2020).

https://thecyberverdict.com/author/emmanuel/

Sinds 2010 zijn er verschillende inbreuken op de cyberbeveiliging gemeld, zelfs door de grootste hotelketens ter wereld:

- Marriott International Hotel Group was verantwoordelijk voor een datalek in 2020 waarbij de persoonlijke gegevens en bekendgemaakte

namen, postadressen, loyaliteitsrekeningnummers en diverse andere gevoelige informatie van klanten niet werden beschermd.

- Ongeveer 340 miljoen gasten waren betrokken bij deze aanval. 2 jaar eerder, in 2018, ontving Marriott een waarschuwing van een interne beveiligingstool met betrekking tot een ongeoorloofde toegangspoging in hun gastenreserveringsdatabase in de Verenigde Staten.
- Nader onderzoek door cyberbeveiligingsexperts wees uit dat ongeautoriseerde toegang tot het reserveringssysteem van het hotel al in 2014 had plaatsgevonden (Secure Stay, 2020).

https://gritdaily.com/marriott-hit-by-second-data-breach-2020/

De gevolgen van cyberdreigingen en/of -aanvallen kunnen de merkreputatie en het consumentenvertrouwen aanzienlijk schaden, met aanzienlijke financiële, juridische en regelgevende gevolgen tot gevolg. Toeristische aanbieders kunnen zowel directe als indirecte financiële verliezen lijden (Paraskevas, 2020) –

- Directe financiële verliezen: bedrijfskosten in verband met IT-hersteldiensten, evenals juridische kosten en PR-diensten.
- Indirecte financiële verliezen: kosten voor het inhuren van extra technisch IT-personeel, het geven van personeelstraining op het gebied van cyberbeveiliging en cyberweerbaarheid, het upgraden van cyberbeveiligingsinfrastructuren, enz.

- Reputatiekosten: als er zich een datalek zou voordoen, zijn er ook reputatiekosten waarmee rekening moet worden gehouden. Reputatiekosten kunnen enorm zijn en leiden tot een daling van het consumentenvertrouwen en boekingen. Toeristische aanbieders moeten hun verantwoordelijkheid erkennen om gegevens en informatie veilig te bewaren om substantiële negatieve gevolgen voor hun bedrijf te voorkomen.

Daarom is het van cruciaal belang voor bedrijven, en met name mkb's, in de reis- en toerismesector om het belang te begrijpen van het implementeren van cyberbeveiliging en cyberweerbaarheid als prioriteiten voor hun bedrijf, in plaats van als een bijzaak.

Post Covid-19-ontwikkelingen

In de nasleep van een wereldwijde pandemie die de toeristenindustrie dwong om online te gaan, moest de reis- en toerismesector hun producten, diensten en consumentenervaringen herdefiniëren om met de nieuwe realiteit om te gaan.

In het post-Covid-19-tijdperk is het aantal cyberdreigingen nog nooit zo hoog geweest.

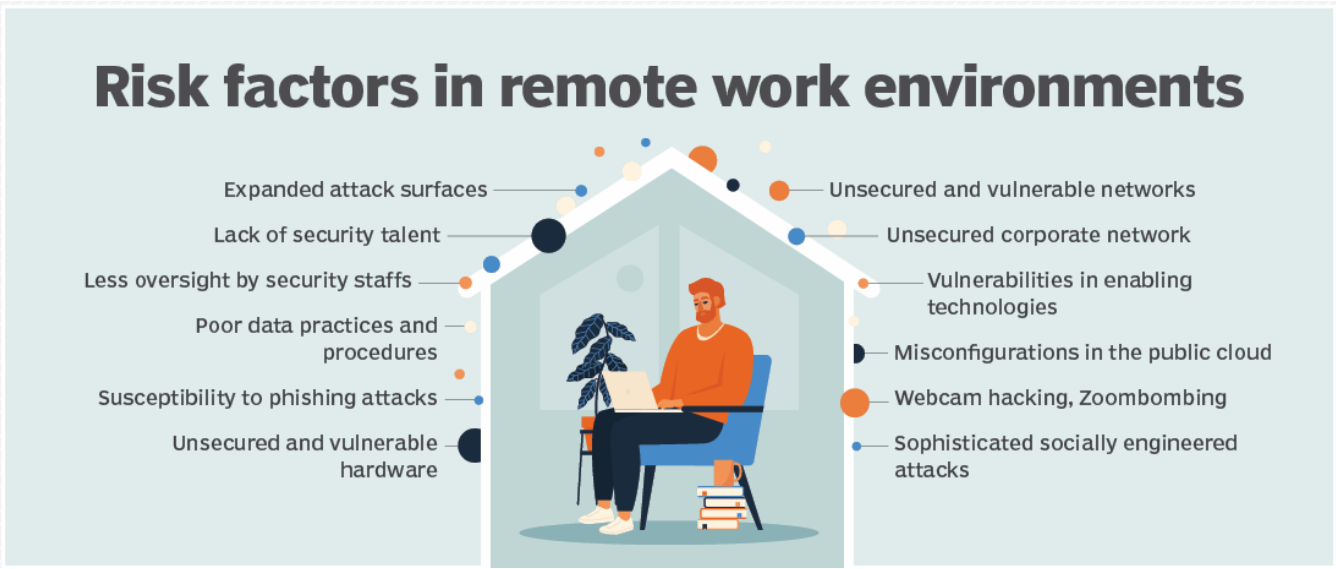
De World Travel & Tourism Council (WTTC) meldt dat de versnelde groei van digitale operaties de sector kwetsbaarder heeft gemaakt en blootgesteld aan cyberrisico's (World Travel & Tourism Council en Microsoft, 2022).

Dit moedigde bedrijven aan om hun beveiligingshouding te herzien om een meer cyberweerbare onderneming op te bouwen en bedrijfseigenaren doen kwaliteitswerk op het gebied van cyberbeveiliging en cyberweerbaarheid.

https://www.idealarticleswriter.com/20__23/03/-Understanding-Digital-Forensics-Process-Techniques-and-Tools-.html

Cyberdreigingsactoren zijn flexibel en zagen Covid-19 als een kans om de kwetsbaarheden van toeristische aanbieders uit te buiten die probeerden reizen te vergemakkelijken en tegelijkertijd de volksgezondheid te beschermen. De voortdurende en inconsistente beperkingen creëerden ruimte voor cyberaanvallen.

De acceptatie van werken op afstand, wat heeft geleid tot een grotere afhankelijkheid van persoonlijke en mobiele apparaten, heeft de verantwoordelijkheid voor de cyberbeveiliging van het bedrijf steeds meer bij werknemers gelegd.



https://www.techtarget.com/searchitoperations/news/365534899/Securin g-remote-access-grows-crucial-for-DevSecOps

Hoewel de cyberecosystemen op locatie van bedrijven over het algemeen veilig zijn, was deze beveiliging voorheen niet uitgebreid tot de huizen van werknemers. Als gevolg hiervan konden aanvallers die toegang kregen tot thuisnetwerken of openbare wifi-netwerken gemakkelijk bedrijfssystemen binnendringen, wat de noodzaak benadrukt van een meer omvattende benadering van cyberbeveiliging - een benadering die de nadruk legt op cyberweerbaarheid.

Hoewel organisaties de veiligheid van thuis- of openbare Wi-Fi-netwerken niet kunnen garanderen, kan personeelstraining helpen om werknemers te beschermen tegen bedreigingen bij het gebruik van IoT-apparaten (Internet of Things).

Cyberdreigingen als gevolg van COVID-19 mogen niet los worden gezien van organisatierisico's, met inbegrip van cyberrisico's die verband houden met hybride wermkbdellen.

Om cyberweerbaarheid te waarborgen, moeten organisaties hun inspanningen voor het monitoren van bedreigingen verbreden om mogelijke

toegangspunten voor aanvallen via thuis- en openbare wifi-systemen te omvatten (World Travel & Tourism Council en Microsoft, 2022).

10.3 Cyberkwetsbaarheid van toeristische mkb's

Hoe kwetsbaar zijn toeristische mkb's?

De WTTC meldt dat meer dan 7 op de 10 (72%) mkb's in het VK, de VS en Europa het slachtoffer zijn geworden van ten minste 1 cyberaanval (World Travel & Tourism Council en Microsoft, 2022).

In de reis- en toerismebranche, die voornamelijk uit het MKB bestaat, zoals reisbureaus en touroperators, ligt het percentage zelfs nog hoger: het MKB is goed voor ongeveer 80% van alle bedrijven.

"Did you know that a cyber-attack happens every 39 seconds and 291 data records are stolen every second?"

https://wisedistribution.co.uk/deception-technology/

Het mkb in het toerisme is de afgelopen jaren een aantrekkelijk doelwit geworden voor cybercriminelen:

- Het hoge niveau van digitaliseringsvolwassenheid maakt het mkb in het toerisme tot een zeer kwetsbare sector op het gebied van cyberbeveiliging en cyberweerbaarheid, met name vanwege de slechte beveiliging van IT en kassasystemen (Fragniere & Yagci, 2021). Volgens Hussain (2023) hebben hackers zich gerealiseerd dat mkb's

gemakkelijker doelwitten zijn in vergelijking met grotere bedrijven met onvoldoende cyberveiligheid, hetzij door een gebrek aan gekwalificeerd en bekwaam personeel (dwz menselijke fouten) of onvoldoende budgetten.

- Toerisme MKB 's zijn bijzonder kwetsbaar voor cyberdreigingen vanwege de zeer gevoelige gegevens en analyses die ze in de cyberruimte opslaan, waardoor het waardevolle informatie wordt voor cybercriminelen die proberen toegang te krijgen tot dergelijke gegevens en deze te schenden, wat leidt tot identiteits- en financiële diefstal, een bedreiging voor gegevensbeheer en bescherming van de privacy van klanten en werknemers (e-mailadressen van klanten, paspoortnummers, creditcardgegevens enz.).
- Het mkb-toerisme is bijzonder gevoelig voor cyberdreigingen, omdat het van nature gefragmenteerd is, waarbij de hele toeleveringsketen (waarbij talloze agenten en externe dienstverleners betrokken zijn) een potentieel toegangsgebied is voor bedreigingsactoren. Proactieve cyberbeveiligingsmaatregelen om de cyberweerbaarheid te waarborgen en een effectieve bedrijfsvoering te behouden, zijn noodzakelijk.

Het Agentschap van de Europese Unie voor cyberbeveiliging (ENISA) ontdekte dat 90% van de mkb's verklaarde dat cyberbeveiligingsproblemen binnen een week nadat de problemen zich voordeden ernstige negatieve gevolgen zouden hebben voor hun bedrijf, en 57% zei dat ze hoogstwaarschijnlijk failliet zouden gaan of failliet zouden gaan van zaken.

https://www.enisa.europa.eu/

Hoe moet de mkb reageren bij een datalek?

In het geval van een datalek wordt de MKB geadviseerd om dit lek te melden aan de commissaris voor informatie en gegevensbescherming en dit online meldingsformulier toe te voegen, uiterlijk 72 uur nadat het zich bewust is geworden van een dergelijk lek.

Als de inbreuk een risico vormt voor de betrokkene, moet de toezichthoudende autoriteit op de hoogte worden gebracht.

Dit zijn 5 concrete acties die een mkb kan ondernemen naar aanleiding van een datalek.

1. Identificeer de bron en de omvang van de inbreuk.
2. Waarschuw jouw taskforce voor inbreuken en pak de inbreuk zo snel mogelijk aan.
3. Test jouw beveiligingsoplossing.
4. Informeer de autoriteiten en alle betrokken klanten.
5. Bereid je voor op het opruimen en beperken van schade na de breuk.

10.4 Cyberdreigingen in het mkb in het toerisme

Wat zijn cyberdreigingen?

Elke omstandigheid of gebeurtenis die mogelijk een negatieve invloed kan hebben op de bedrijfsvoering, activa, werknemers en/of andere organisaties, of een land via een systeem via ongeautoriseerde toegang, vernietiging, openbaarmaking, wijziging van informatie en/of denial of service.

Er zijn 3 hoofdtypen cyberdreigingen:

1. Cybercriminaliteit omvat afzonderlijke actoren of groepen die zich op systemen richten voor financieel gewin of om verstoringen te veroorzaken.
2. Bij een cyberaanval wordt vaak politiek gemotiveerde informatie verzameld.
3. Cyberterrorisme is bedoeld om elektronische systemen te ondermijnen om paniek of angst te veroorzaken.

Wat zijn de belangrijkste soorten cyberdreigingen in het mkb in het toerisme?

Als het gaat om pogingen tot cyberdreiging, zijn mkb's in de reis- en toerismesector wereldwijd een van de meest getroffen sectoren.

Cyberaanvallen in de reissector zijn voornamelijk gericht op creditcards, persoonlijk identificeerbare informatie, beloningsprogramma's voor gastvrijheid en openbaar beschikbaar internet (Walson, 2022).

In een PwC Hotel Outlook Report van 2018 tot 2022 stond dat de hotelbranche na de Retail sector het maximale aantal datalekken had.

Volgens de WTTC blijven phishing-, malware- en ransomware-bedreigingen constant, waarbij ransomware in 2021 verantwoordelijk is voor 23% van de cyberaanvallen en phishing bij 33% van de cyberaanvallen. Cybercriminelen krijgen grotendeels toegang tot cyberomgevingen via phishing, diefstal van inloggegevens of remote desktop control (World Travel & Tourism Council en Microsoft, 2022).

https://motyl-szary.co m/2023/03/31/top-cybersecurity-threats-and-proactive-measures-to-protect-personal-and-business-data/

De meest gebruikelijke methoden die worden gebruikt door kwaadwillende actoren wanneer ze proberen de cyberbeveiliging en cyberweerbaarheid van een toerismebedrijf te bedreigen -

- Malware: dit is een van de meest voorkomende cyberdreigingen die wordt verspreid via een ongevraagde e-mailbijlage of legitiem ogende download. Malware-aanvallen brengen de gevoelige systemen en gegevens van een organisatie in gevaar door ze te infecteren met kwaadaardige software zoals virussen, wormen, Trojaanse paarden en andere spyware (Paraskevas, 2020).
- Phishing: dit is altijd het meest voorkomende type cyberaanval geweest en vindt vaak plaats via e-mail. Het vindt plaats wanneer

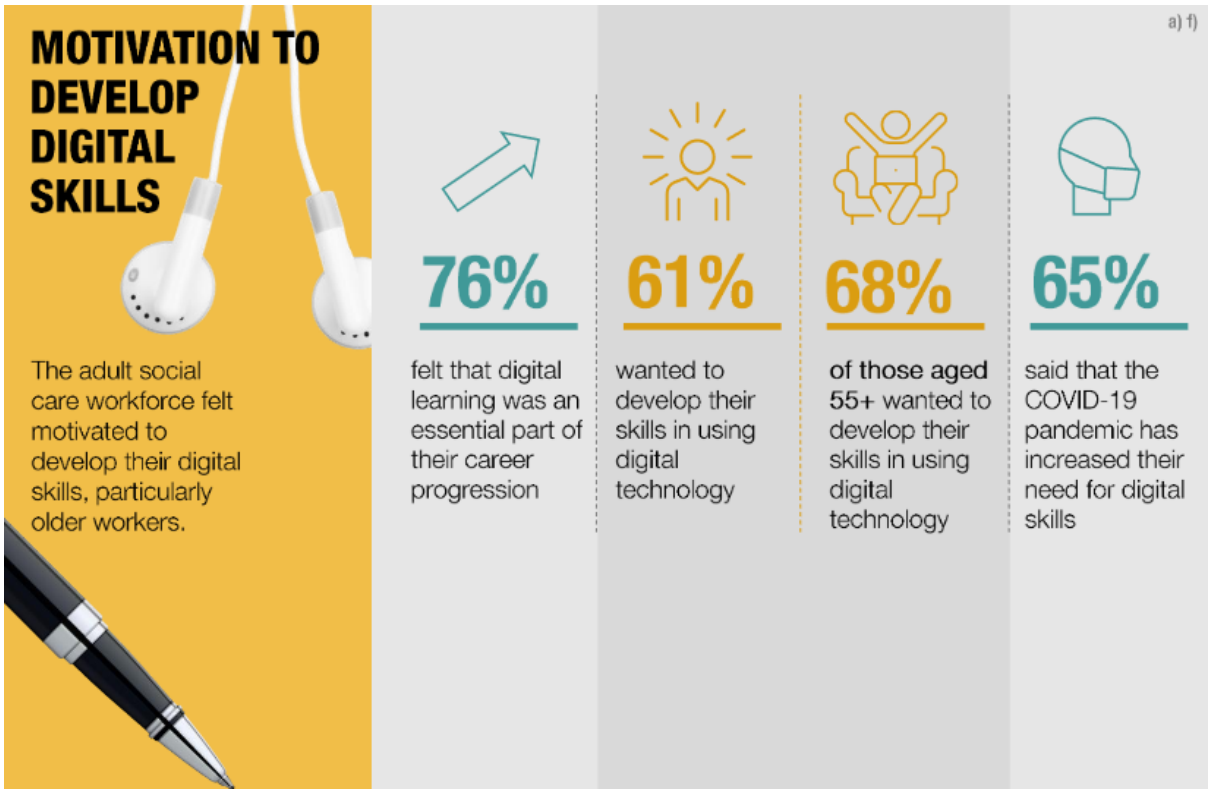
cybercriminelen e-mails sturen naar slachtoffers die afkomstig lijken te zijn van een legitiem bedrijf (bijvoorbeeld een bank) en om gevoelige informatie vragen (bijvoorbeeld bankrekeninggegevens, wachtwoorden).

- Point-of-sale (POS)-aanvallen: komen ook veel voor in de reis- en toerismesector en geven aanvallers waardevolle gegevens, waaronder creditcardgegevens zoals kaartnummers en persoonlijke identificatienummers (PIN's).
- Man-in-the-middle: dit type cyberaanval vindt plaats op een onbeveiligd wifi- netwerk waar een bedreigingsacteur gegevens kan onderscheppen die worden doorgegeven vanaf het apparaat van het slachtoffer en het netwerk.
- Ransomware: het doel van deze dreiging is niet om gegevens te stelen, maar om de eigenaar de toegang ertoe te ontzeggen en het doelwit de aanvaller rechtstreeks te laten betalen. Ransomware is geprogrammeerd om de meest gevoelige of waardevolle gegevens van het bedrijf te identificeren.
- Botnetaanvallen: gebruik van grote netwerken, vaak bestaande uit talloze computers, smartphones of intelligente apparaten (ook wel 'zombielegers' genoemd) voor het uitvoeren van kwaadaardige activiteiten zoals inlogpogingen, spamaanvallen of het uitschakelen van netwerken, netwerkapparaten, websites of de IT-omgeving van een organisatie.
- Aanvallen op externe serviceproviders: bedreigingsactoren richten zich ook op leden van de ' DexteR ' van de organisatie (digitale partners en externe serviceproviders) – deze worden vaak beschouwd als de zwakkere schakels in het netwerk en vormen aantrekkelijke verzamelpunten voor gevoelige bedrijfsgegevens (IBM 2018 zoals geciteerd in Paraskevas, 2020).

10.5 Goede cyberpraktijken voor mkb-toeristen

Een cruciaal onderdeel van cyberbeveiliging en cyberweerbaarheid is **het bieden van opleiding aan het personeel en het trainen van digitale vaardigheden.** Werknemers die goed zijn opgeleid om te voorkomen dat ze

het slachtoffer worden van cyberaanvallen en weten wat ze moeten melden, kunnen de beveiligingssystemen van een toeristische mkb verbeteren en het risico op cyberdreigingen verminderen, zoals ongeoorloofde toegang tot de cybersystemen van het bedrijf.



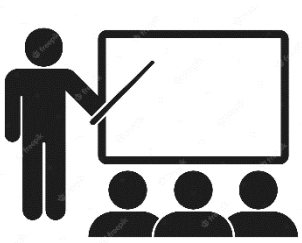
https://www.digitalsocialcare.co.uk/digital-skills-and-training/

De WTTC identificeert 7 good practices die genomen kunnen worden om de cyberweerbaarheid verder te vergroten:

1. Integreer cyberrisicobeheer in organisatorisch risicobeheer

Cyberrisico's moeten worden geprioriteerd en samen met andere zakelijke en operationele risico's worden beheerd. Bedrijven moeten hun risicobeheerprocessen regelmatig herzien en bijwerken en een budget toewijzen op basis van het risiconiveau en de vereiste risicobeperkende maatregelen. Bekwame medewerkers zijn nodig om cyberrisicobeleid te creëren en te informeren, best practices te implementeren en risico's proactief en continu te beheren.

2. Alle medewerkers opleiden en trainen



Training is cruciaal voor de introductie van nieuw personeel en voor het opleiden van huidig personeel om een effectief gebruik van digitale systemen en processen en veiligheid te waarborgen. Hoewel niet alle werknemers hetzelfde opleidingsniveau nodig hebben, is het belangrijk dat het personeel een fundamenteel begrip heeft van cyberbeveiligingsprincipes. Dit verkleint de kans op cyberaanvallen door insiders.

https://www.freepik.com/premium-vector/training-icon-vector-training-education-icon-blackboard

3. Breid risicobescherming uit tot buiten de fysieke werkplek

Met de overgang naar werken op afstand en hybride werken, moeten cybercontroles breder worden toegepast. Het is van cruciaal belang om na te gaan hoe hybride werkmodellen de beveiliging kunnen beïnvloeden en kwetsbaarheden kunnen vergroten, waaronder wifi-beveiliging thuis, cyberhygiëne van werknemers op hun eigen apparaten, enz.

https://pbosecure.com/blogs/apply-zero-trust-information-security-framework-to-icsot-environment

4. Gebruik een zero-trustbenadering voor cyberbeveiliging

De zero-trust-benadering wijkt af van eerdere methoden die vertrouwden op een hoger niveau van vertrouwen binnen de organisatie. Het is gebaseerd op expliciete verificatie van toegangsverzoeken, toegang met minimale bevoegdheden en gaat uit van een inbreuk of compromis. Dit maakt meer flexibiliteit in toegang mogelijk terwijl de blootstelling aan kernsystemen wordt beperkt.

5. Maak gebruik van doorlopende dreigingsevaluaties

Dit omvat het versterken van de weerbaarheid tegen cyberdreigingen door relaties op te bouwen met experts in het veld, analyses te gebruiken om beschermingsmaatregelen te verfijnen, penetratietesten uit te voeren om kwetsbaarheden te identificeren,

systemen te segmenteren om de impact van inbreuken te beperken en prioriteit te geven aan de bescherming van systemen.

https://www.clipartmax.com/middle/m2H7i8G6K9m2A0Z5_a-checklist-with-a-warning-sign-to-depict-risk-identification-risk-assessment/

6. Wees transparant

Het is essentieel om geïmplementeerde beveiligingsmaatregelen en de redenen voor gegevensverzameling, gegevensgebruik en gegevensopslagperioden te communiceren. Mkb-bedrijven in de toeristische sector mogen alleen de minste hoeveelheid persoonsgegevens en betalingsinformatie verzamelen die nodig is en de hoogste niveaus van bescherming bieden om het vertrouwen te bevorderen. Naleving van wetgeving en normen (bijv. GDPR) moet worden benadrukt. Als er zich een inbreuk voordoet, moeten de betrokken partijen en regelgevende instanties onmiddellijk op de hoogte worden gebracht en moeten er maatregelen worden genomen om de gevolgen van de inbreuk te beperken.

7. Implementeer een organisatiestandaard

Zakelijke leiders moeten voldoen aan de wetgeving in de regio's waar hun organisatie actief is. De missie van de EU om een gestandaardiseerde benadering van cyberbeveiliging en -weerbaarheid en gegevensbescherming te bevorderen, heeft geleid tot de ontwikkeling van:

- De EU-wet over cyberweerbaarheid heeft tot doel gemeenschappelijke cyberbeveiligingsregels vast te stellen voor digitale producten en bijbehorende diensten die op de EU-markt worden gebracht.
- De EU-cyberbeveiligingswet versterkt de ENISA en stelt een cyberbeveiligingscertificeringskader voor producten en diensten vast.
- Het evoluerende cyberlandschap vereist specifieke cyberwetten om de civiele bescherming te verbeteren; hier komt de Algemene Verordening Gegevensbescherming (AVG) van de EU om de hoek kijken. De huidige prioriteit van ENISA is het aanmoedigen van gegevensbeschermingsmaatregelen om te laten zien hoe cyberbeveiligingstechnologieën de naleving van de gegevensbeschermingsbeginselen van de AVG kunnen ondersteunen

(zie de stappen met betrekking tot de reactie op datalekken in Sectie 10.3).

- Op 18 april 2023 een mededeling over een academie voor cyberbeveiligingsvaardigheden aangenomen.

  Dergelijke regelgeving en beleidsinitiatieven moeten door mkb-toeristen in overweging worden genomen bij het ontwikkelen en implementeren van een organisatiestandaard, die ook moet worden geïnformeerd door deskundigen op het gebied van cyberbeveiliging, privacy en juridische zaken.

De ENISA heeft een cyberbeveiligingsgids voor het mkb ontwikkeld waarin 12 stappen worden belicht waarmee het mkb zijn bedrijf kan beveiligen.

De stappen zijn:

1. Ontwikkel een goede cyberveiligheidscultuur;
2. Zorg voor een passende opleiding;
3. Zorgen voor effectief beheer door derden;
4. Ontwikkel een incidentresponsplan;
5. Beveiligde toegang tot systemen;
6. Beveiligde apparaten;
7. Beveilig het netwerk;
8. Verbeter de fysieke beveiliging;
9. Veilige back-ups;
10. Ga aan de slag met de cloud;
11. Beveiligde onlinesites;
12. Zoek en deel informatie;

https://ecs-org.eu/enisa-introduces-the-european-cybersecurity-skills-framework/

10.6 Conclusie

- In deze module werd gekeken naar de manieren waarop cyberbeveiliging en cyberweerbaarheid een sleutelrol spelen in de bedrijfsvoering van de toeristische sector, de problemen en risico's van cyberaanvallen en goede praktijken.
- Digitale vaardigheden kunnen dienen als een instrument voor de toeristische sector om beter te begrijpen hoe cyberbeveiliging en cyberweerbaarheod de sector vormgeven en om plannen te maken voor een veiligere toekomst.
- Het omarmen van beveiliging en weerbaarheid als een normale manier van het cyberleven van het bedrijf is in het algemeen belang.

10.7 Lezen en aanvullend materiaal

Verder lezen

https://link.springer.com/chapter/10.1007/978-3-319-16486-1_31
https://www.ttgmedia.com/news/news/smes-at-greatest-risk-of-cyber-attacks-says-wttc-33908

https://digitalcommons.usf.edu/m3publishing/vol17/iss9781732127593/7/

https://link.springer.com/referenceworkentry/10.1007/978-3-030-05324-6_100-1

https://securestay.medium.com/the-history-of-hotels-cyber-attacks-4b6a09c8bf30 _

https://www.ten-inc.com/presentations/Symantec-The-Cyber-Resilience-Blueprint.pdf

https://wttc.org/Portals/0/Documents/Reports/2022/WTTC_x_Microsoft-Codes_To_Resilience.pdf

https://idpc.org.mt/report-a-breach/

https://www.whoa.com/5-ste ps-to-take-after-a-small-business-data-breach/

Websites

https://digital-skills-jobs.europa.eu/en/cybersecurity-skills-academy
https://www.enisa.europa.eu/topics/cybersecurity-education/sme_cybersecurity
https://www.enisa.europa.eu/publications/cybersecurity-guide-for-smes/@@download/fullReport _
https://www.enisa.europa.eu/topics/cybersecur ity-policy/data-protection
https://www.eurotechconseil.com/en/blog/difference-between-cyber-security-and-cyber-resilience/ _
https://www.goallsecure.com/cyber-security-in-travel/
https://www.i-scoop.eu/cybersecurity/cyber-resilience/

https://mbb.org.mt/wp-content/uploads/2022/12/CRA-Brief-.pdf
https://www.omnicybersecurity.com/cyber-attacks-travel-tourism-industry/
https://www.techtarget.com/what is/definition/Confidentiality-integrity-and-availability-CIA
https://www.wcrcentre.co.uk /post/why-should-cyber-security-matter-to-an-SME-in-the-tourism-and-hospitality-industry

Youtube filmpjes

https://www.youtube.com/watch?v=z5nc9MDbvkw

https://www.youtube.com/watch?v=JbEPJv7Ybcs

https://www.youtube.com/watch?v=inWWhr5tnEA _