CYBERSECURITY VOOR
HET MKB

tien

CYBERSECURITY BASICS

Cybercriminelen vallen organisaties van alle groottes aan

Als je enkele cybersecurity basics kent en ze in praktijk brengt, kan je jouw bedrijf beschermen en het risico van een cyberaanval verkleinen.

BESCHERM
JE DATA & DEVICES

Update je software

Dit geldt ook voor jouw apps, webbrowsers en besturingssystemen. Stel in dat updates automatisch plaatsvinden.

Beveilig je bestanden

Maak een back-up van belangrijke bestanden offline, op een externe harde schijf of in de cloud. Zorg er ook voor dat je jouw papieren bestanden veilig bewaart.

Wachtwoorden vereist

Gebruik wachtwoorden voor alle laptops, tablets en smartphones. Laat deze apparaten niet onbeheerd achter op openbare plaatsen.

Versleutel je devices

Versleutel apparaten en andere media die gevoelige persoonlijke informatie bevatten. Hieronder vallen laptops, tablets, smartphones, verwisselbare schijven, back-upbanden en cloudopslagoplossingen.

Gebruik multi-factor authenticatie

Eis multi-factor authenticatie voor toegang tot delen van het netwerk met gevoelige informatie. Dit vereist extra stappen naast het inloggen met een wachtwoord - zoals een tijdelijke code op een smartphone of een hardware sleutel die in een computer wordt gestoken.

MEER WETEN?
tiensecurity.nl

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

CYBERSECURITY VOOR
HET MKB

tien

BEVEILIG JE DRAADLOOS NETWERK

Beveilig je router

Wijzig de standaardnaam en het standaardwachtwoord, schakel beheer op afstand uit en log uit als beheerder zodra de router is ingesteld.

Gebruik ten minste WPA2-codering

Zorg ervoor dat jouw router WPA2- of WPA3-encryptie biedt en dat deze is ingeschakeld. Encryptie beschermt informatie die via jouw netwerk wordt verzonden, zodat deze niet door buitenstaanders kan worden gelezen.

MAAK SMART SECURITY BUSINESS AS USUAL

Sterke wachtwoorden vereist

Een sterk wachtwoord bestaat uit minstens 12 tekens die een mix is van cijfers, symbolen en hoofdletters. Gebruik wachtwoorden nooit opnieuw en deel ze niet via de telefoon, sms of e-mail. Beperk het aantal mislukte inlogpogingen om wachtwoord-gluur-aanvallen te beperken.

Train je collega's

Creëer een beveiligingscultuur door een regelmatig trainingsschema voor werknemers te implementeren. Breng medewerkers op de hoogte van nieuwe risico's en kwetsbaarheden. Als werknemers niet deelnemen, overweeg dan hun toegang tot het netwerk te blokkeren.

Maak een plan

Maak een plan voor het opslaan van gegevens, het runnen van het bedrijf en het informeren van klanten als u te maken krijgt met een inbreuk.

MEER WETEN?
tiensecurity.nl

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

CYBERSECURITY VOOR
HET MKB

tien

Het begrijpen van

HET NIST CYBERSECURITY FRAMEWORK

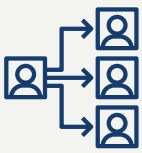
Het NIST Cybersecurity Framework, maar wat is het precies?

En is het op jou van toepassing? NIST is het National Institute of Standards and Technology van het Amerikaanse Ministerie van Handel. Het NIST Cybersecurity Framework helpt bedrijven van elke omvang hun cyberbeveiligingsrisico's beter begrijpen, beheren en beperken en hun netwerken en gegevens beschermen.

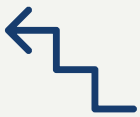
Het Framework is vrijwillig. Het geeft uw bedrijf een overzicht van best practices om u te helpen beslissen waar u uw tijd en geld voor cyberbeveiligingsbescherming op wilt richten. U kunt het NIST Cybersecurity Framework in uw bedrijf toepassen op deze vijf gebieden: Identificeren, Beschermen, Detecteren, Reageren en Herstellen.

1. IDENTIFY

Maak een lijst van alle apparatuur, software en gegevens die je gebruikt, waaronder laptops, smartphones, tablets en apparaten voor verkooppunten. Stel een bedrijfsbeleid inzake cyberbeveiliging op en deel dit met anderen:



Rollen en verantwoordelijkheden voor werknemers, verkopers en anderen met toegang tot gevoelige gegevens.



Te nemen stappen ter bescherming tegen een aanval en ter beperking van de schade als zich een aanval voordoet.

2. PROTECT

- Controleer wie op uw netwerk inlogt en uw computers en andere apparaten gebruikt.
- Gebruik beveiligingssoftware om data te beschermen.
- Versleutel gevoelige gegevens
- Maak regelmatig back-ups van de data.
- Update beveiligingssoftware regelmatig en automatiseer deze updates indien mogelijk.
- Een formeel beleid hebben voor het veilig verwijderen van elektronische data en oude apparaten.
- Train iedereen die jouw computers, apparaten en netwerk gebruikt over cyberbeveiliging. Je kunt werknemers helpen hun persoonlijke risico's te begrijpen, naast hun cruciale rol op de werkplek.

MEER WETEN?
tiensecurity.nl

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

CYBERSECURITY VOOR
HET MKB

tien

3. DETECT

Controleer computers op toegang door onbevoegd personeel, apparaten (zoals USB-sticks) en software.

Controleer jouw netwerk op ongeautoriseerde gebruikers of verbindingen.

Onderzoek alle ongewone activiteiten op jouw netwerk of door jouw personeel.

4. RESPOND

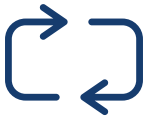
Maak een plan voor:

- Klanten, werknemers en anderen wiens gegevens mogelijk gevaar lopen op de hoogte brengen.
- De bedrijfsvoering gaande houden.
- De aanval melden aan de politie en andere autoriteiten.
- Het onderzoeken en inperken van een aanval.
- Je cyberbeveiligingsbeleid en -plan bijwerken aan de hand van geleerde lessen.
- Voorbereiding op onbedoelde gebeurtenissen (zoals noodweer) die gegevens in gevaar kunnen brengen.

Test je plan regelmatig!

5. RECOVER

Na een aanval:



Reparatie en herstel van de apparatuur en delen van uw netwerk die zijn aangetast.

Houd werknemers en klanten op de hoogte van de reactie- en herstelactiviteiten.

MEER WETEN?
tiensecurity.nl

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

CYBERSECURITY VOOR
HET MKB

tien

FYSIEKE SECURITY

Cyberbeveiliging begint met sterke fysieke beveiliging.

Gaten in de fysieke beveiliging kunnen gevoelige bedrijfsgegevens blootstellen aan identiteitsdiefstal, met mogelijk ernstige gevolgen. Bijvoorbeeld:

Een werknemer laat per ongeluk een flash drive achter op een koffiehuis tafel. Wanneer hij uren later terugkomt om het te halen, is de schijf - met honderden opgeslagen sofinummers - verdwenen. Een andere werknemer gooit stapels oude bankgegevens in een vuilnisbak, waar een crimineel ze na werktijd vindt.
Een inbreker steelt bestanden en computers uit uw kantoor nadat hij door een niet afgesloten raam is binnengekomen.

HOE BESCHERM JE APPARATUUR & PAPIER

Hier volgen enkele tips voor het beschermen van informatie in papieren dossiers en op harde schijven, flash drives, laptops, betaalautomaten en andere apparatuur.

Sla veilig op

Wanneer papieren dossiers of elektronische apparaten gevoelige informatie bevatten, bewaar ze dan in een afgesloten kast of kamer.

Fysieke toegang beperken

Wanneer dossiers of apparaten gevoelige gegevens bevatten, geef dan alleen toegang aan degenen die ze nodig hebben.

Stuur reminders

Herinner werknemers eraan papieren bestanden in afgesloten archiefkasten te stoppen, uit te loggen bij uw netwerk en toepassingen, en nooit bestanden of apparaten met gevoelige gegevens onbeheerd achter te laten.

Houd bij

Houd alle apparaten die gevoelige klantgegevens verzamelen bij en beveilig ze. Bewaar alleen bestanden en gegevens die je nodig hebt en weet wie er toegang toe heeft.

MEER WETEN?
tiensecurity.nl

CYBERSECURITY VOOR
HET MKB

tien

HOE BESCHERM JE DATA OP JE DEVICES

Een inbraak, verloren laptop, gestolen mobiele telefoon of zoekgeraakte flashdrive - het kan allemaal gebeuren door gebreken in de fysieke beveiliging. Maar de kans op een datalek is kleiner als de informatie op die apparaten wordt beschermd. Hier zijn een paar manieren om dat te doen:

Complexe wachtwoorden vereist

Eis wachtwoorden die lang, complex en uniek zijn. En zorg ervoor dat deze wachtwoorden veilig worden opgeslagen. Overweeg het gebruik van een wachtwoordmanager.

Gebruik multi-factor authenticatie

Eis multi-factor authenticatie voor toegang tot delen van uw netwerk met gevoelige informatie. Dit vereist extra stappen naast het inloggen met een wachtwoord - zoals een tijdelijke code op een smartphone of een sleutel die in een computer wordt gestoken.

Beperkt inlogpogingen

Beperk het aantal foutieve aanmeldingspogingen dat is toegestaan om apparaten te ontgrendelen. Dit zal helpen beschermen tegen indringers.

Versleutel

Versleutel draagbare media, waaronder laptops en USB-sticks, die gevoelige informatie bevatten. Versleutel alle gevoelige gegevens die je buiten het bedrijf verstuurt, bijvoorbeeld naar een accountant of een verzenddienst.

TRAIN JE COLLEGA'S

Neem fysieke beveiliging op in je reguliere trainingen en communicatie met werknemers. Herinner werknemers eraan om:

Versnipper documenten

Versnipper documenten met gevoelige informatie altijd voordat je ze weggooit.

Verwijder data correct

Gebruik software om gegevens te wissen voordat je oude computers, mobiele apparaten, digitale kopieerapparaten en schijven doneert of weggooit. Vertrouw niet op "wissen" alleen.

Bevorderen van beveiliging op alle locaties

Beveiliging handhaven, zelfs als je op afstand thuis of op zakenreis werkt.

Weet het respons plan

Al het personeel moet weten wat te doen bij verlies of diefstal van apparatuur of papieren dossiers, inclusief wie te waarschuwen en wat vervolgens te doen. Gebruik Data Breach Response: A Guide for Business voor hulp bij het opstellen van een responsplan.

MEER WETEN?
tiensecurity.nl

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

CYBERSECURITY VOOR
HET MKB

tien

RANSOMWARE

Iemand in jouw bedrijf krijgt een e-mail

Het ziet er legitiem uit, maar met één klik op... een link, of een download van een bijlage, is iedereen buitengesloten van je netwerk. Die link downloadde software die jouw gegevens gijzelt. Dat is een ransomware aanval.

De aanvallers vragen om geld of cryptocurrency, maar zelfs als je betaalt, weet je niet of de cybercriminelen jouw gegevens zullen bewaren of jouw bestanden zullen vernietigen. Ondertussen zijn de informatie die je nodig hebt om jouw bedrijf te runnen en gevoelige gegevens over jouw klanten, werknemers en bedrijf nu in criminele handen. Ransomware kan een serieuze tol eisen van jouw bedrijf.

HOE HET GEBEURD

Criminelen kunnen op verschillende manieren een ransomware-aanval starten.

Scam e-mails

met links en bijlagen die jouw gegevens en netwerk in gevaar brengen. Deze phishing-e-mails vormen de meeste ransomware-aanvallen.

Server vulnerabilities

waar hackers misbruik van kunnen maken.

Geinfecteerde websites

die automatisch kwaadaardige software downloaden naar uw computer.

Online ads

die kwaadaardige code bevatten - zelfs op websites die je kent en vertrouwt.

MEER WETEN?
tiensecurity.nl

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

CYBERSECURITY VOOR
HET MKB

tien

HOE BESCHERM JE JOUW BEDRIJF

Heb een plan

Hoe blijft jouw bedrijf staande na een ransomware-aanval?
Zet dit plan op papier en deel het met iedereen die het moet weten.

Maak back-ups

Sla regelmatig belangrijke bestanden op een schijf of server op die niet op jouw netwerk is aangesloten. Maak de back-up van gegevens onderdeel van jouw routinematige bedrijfsvoering.

Houd je security up-to-date

Installeer altijd de laatste patches en updates. Zoek naar aanvullende beschermingsmaatregelen, zoals zoals e-mailverificatie en inbraakpreventiesoftware, en stel deze in om automatisch te worden bijgewerkt op jouw computer. Op mobiele apparaten moet je dit mogelijk handmatig doen.

Security bewustzijn

Leer je collega's hoe ze phishing-zwendel kunnen vermijden en toon hen enkele veel voorkomende manieren waarop computers en apparaten worden geïnfecteerd. Neem tips voor het herkennen en beschermen tegen ransomware op in de reguliere oriëntatie en training.

WAT TE DOEN ALS JE BENT GEHACKED

Beperk de schade

Koppel de geïnfecteerde computers of apparaten onmiddellijk los van het netwerk. Als jouw gegevens zijn gestolen, neem dan maatregelen om jouw bedrijf te beschermen en stel degenen die hierdoor kunnen worden getroffen op de hoogte.

Bel de politie

Meld de aanval meteen bij de politie en doe aangifte.

Houd je bedrijf gaande

Nu is het tijd om dat plan uit te voeren. Een back-up van de gegevens zal helpen.

Moet ik betalen?

De politie raadt dat niet aan, maar het is aan jou om te bepalen of de risico's en kosten van het betalen de mogelijkheid om jouw bestanden terug te krijgen waard zijn. Het betalen van losgeld is echter geen garantie dat je de gegevens terugkrijgt.

Informeer je klanten

Als gegevens of persoonlijke informatie zijn gecompromitteerd, zorg er dan voor dat je de getroffen partijen op de hoogte brengt - zij kunnen het risico lopen op identiteitsdiefstal. Informatie over hoe je dat moet doen in het Data Breach Response: Een gids voor bedrijven.

MEER WETEN?
tiensecurity.nl

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

CYBERSECURITY VOOR
HET MKB

tien

PHISHING

Je krijgt een e-mail die lijkt te komen van iemand die je kent.

Het lijkt van een van de leveranciers van uw bedrijf te komen en vraagt je op een link te klikken om jouw bedrijfsaccount bij te werken. Moet je klikken? Misschien lijkt het alsof het van je baas komt en vraagt het om je netwerkwachtwoord. Moet je antwoorden? In beide gevallen waarschijnlijk niet. Dit kunnen phishingpogingen zijn.

HOE

PHISHING WERKT

Je krijgt een e-mail of sms

Het lijkt van een bekende te zijn, en het vraagt je op een link te klikken, of je wachtwoord, zakelijke bankrekening of andere gevoelige informatie te geven.

Het lijkt echt

Het is gemakkelijk om logo's te vervalsen en valse e-mailadressen te verzinnen. Oplichters gebruiken bekende bedrijfsnamen of doen zich voor als een bekende.

Het is belangrijk

Het bericht zet je onder druk om nu te handelen - of er zal iets ergs gebeuren.

Wat er gebeurt

Als u op een link klikt, kunnen scammers ransomware of andere programma's installeren die je van jouw gegevens afsluiten en zich verspreiden naar het hele bedrijfsnetwerk. Als je wachtwoorden deelt, hebben scammers nu toegang tot al die accounts.

WAT JIJ KAN DOEN

Voordat je op een link klikt of gevoelige bedrijfsinformatie deelt:

Check het

Zoek de website of het telefoonnummer op van het bedrijf of de persoon achter de tekst of e-mail. Zorg ervoor dat je het echte bedrijf krijgt en niet op het punt staat malware te downloaden of met een oplichter te praten.

Praat met iemand

Een gesprek met een collega kan helpen uit te zoeken of het verzoek echt is of een phishingpoging.

Bel als je niet zeker bent

Pak de telefoon en bel die verkoper, collega of klant die de e-mail heeft gestuurd. Bevestig dat ze echt informatie van je nodig hebben. Gebruik een nummer waarvan je weet dat het correct is, niet het nummer in de e-mail of tekst.

MEER WETEN?
tiensecurity.nl

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

CYBERSECURITY VOOR
HET MKB

tien

HOE BESCHERM JE JOUW BEDRIJF

Maak back-ups

Maak regelmatig een back-up van gegevens en zorg ervoor dat die back-ups niet verbonden zijn met het netwerk. Als een phishing-aanval plaatsvindt en hackers toegang krijgen tot het netwerk, kan je op die manier gegevens herstellen.

Houd je security up-to-date

Installeer altijd de nieuwste patches en updates. Zoek naar aanvullende beschermingsmaatregelen, zoals e-mailverificatie en preventiesoftware, en stel deze zo in dat ze automatisch worden bijgewerkt. Op mobiele apparaten moet je dit wellicht handmatig doen.

Waarschuw je collega's

Deel deze informatie met hen. Onthoud dat phishing-zwendelaars hun tactieken vaak veranderen, dus zorg ervoor dat je in jouw reguliere training tips opneemt om de nieuwste phishing-schema's te herkennen.

Een vangnet inzetten

Gebruik technologie voor e-mailverificatie om te voorkomen dat phishing-e-mails de inbox van jouw bedrijf bereiken.

WAT ALS JE WEL KLIKT IN EEN PHISHING MAIL

Waarschuw anderen

Praat met uw collega's en deel uw ervaringen. Phishing-aanvallen overkomen vaak meer dan één persoon in een bedrijf.

Beperk de schade

Wijzig onmiddellijk alle gecompromitteerde wachtwoorden en koppel computers of apparaten die met malware zijn besmet los van het netwerk.

Volg de procedures van je bedrijf

Dit kan inhouden dat u specifieke mensen in jouw organisatie of aannemers die je helpen met IT.

Meld het je klanten

Als jouw gegevens of persoonlijke informatie zijn gecompromitteerd, zorg er dan voor dat je de betrokken partijen op de hoogte brengt - zij kunnen het risico lopen van identiteitsdiefstal.

Meld het

Stuur phishing-e-mails door naar reportphishing@apwg.org (een adres dat wordt gebruikt door de Anti-Phishing Working Group, die ISP's, beveiligingsbedrijven, financiële instellingen en wetshandhavingsinstanties omvat). Breng het bedrijf of de persoon die zich voordeed op de hoogte van het phishingprogramma.

MEER WETEN?
tiensecurity.nl

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

CYBERSECURITY VOOR
HET MKB

tien

ZAKELIJKE E-MAIL OPLICHTERS

Een oplichter zet een e-mail adres op dat lijkt alsof het van jouw bedrijf komt.

Vervolgens verstuurt de oplichter berichten via dat e-mailadres. Deze praktijk heet spoofing, en de oplichter is wat wij noemen een zakelijke e-mail oplichter.

Oplichters doen dit om wachtwoorden en bankrekeningnummers te bemachtigen of om iemand geld te laten sturen. Wanneer dit gebeurt, heeft jouw bedrijf veel te verliezen. Klanten en partners kunnen hun vertrouwen verliezen en hun zaken elders doen - en jouw bedrijf kan dan geld verliezen.

HOE BESCHERM JE JOUW BEDRIJF

Gebruik e-mailverificatie

Wanneer je de e-mail van jouw bedrijf instelt, moet je ervoor zorgen dat de e-mailprovider e-mailverificatietechnologie biedt. Als je dan een e-mail verstuurt vanaf de server van jouw bedrijf, kunnen de ontvangende servers bevestigen dat de e-mail echt van jou afkomstig is. Als dat niet het geval is, kunnen de ontvangende servers de e-mail blokkeren en een bedrieglijke zakelijke e-mail afleiden.

Houd de beveiliging up-to-date

Installeer altijd de laatste patches en updates. Stel ze zo in dat ze automatisch worden bijgewerkt op jouw netwerk. Zoek naar aanvullende beschermingsmiddelen, zoals inbraakpreventiesoftware, die jouw netwerk controleert op verdachte activiteiten en je waarschuwt als het die vindt.

Train je collega's

Leer ze hoe ze phishing-scams kunnen vermijden en laat ze enkele van de veelvoorkomende manieren zien waarop aanvallers computers en apparaten met malware kunnen infecteren. Neem tips voor het opsporen van en bescherming tegen cyberdreigingen op in de reguliere trainingen en communicatie voor werknemers.

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

CYBERSECURITY VOOR
HET MKB

tien

WAT TE DOEN

ALS IEMAND DE E-MAIL VAN JOUW BEDRIJF VERVALST

Meld het

Meld het bij de politie. Je kunt phishing-e-mails ook doorsturen naar naar reportphishing@ apwg.org (een adres dat wordt gebruikt door de Anti-Phishing Working Group, waarin ISP's, beveiligingsleveranciers, financiële instellingen en wetshandhavingsinstanties zijn vertegenwoordigd).

Informeer je klanten

Als je ontdekt dat oplichters zich voordoen als jouw bedrijf, vertel dit dan zo snel mogelijk aan jouw klanten - per post, e-mail of sociale media. Als je jouw klanten een e-mail stuurt, stuur dan een e-mail zonder hyperlinks. Je wilt niet dat jouw kennisgevingsmail lijkt op een phishing-scam. Herinner klanten eraan geen persoonlijke informatie te delen via e-mail of sms.

Waarschuw je collega's

Gebruik deze ervaring om jouw beveiligingspraktijken bij te werken en jouw personeel op te leiden over cyberdreigingen.

MEER WETEN?
tiensecurity.nl

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

CYBERSECURITY VOOR
HET MKB

tien

TECH SUPPORT SCAMS

Je krijgt een telefoontje, pop-up of e-mail waarin staat dat er een probleem is met jouw computer.

Vaak zitten oplichters achter deze telefoontjes, pop-upberichten en e-mails. Ze willen jouw geld, persoonlijke informatie of toegang tot jouw bestanden. Dit kan het netwerk beschadigen, gegevens in gevaar brengen en jouw bedrijf schaden.

HOE DE SCAM WERKT

De oplichters kunnen doen alsof ze van een bekend techbedrijf zijn, zoals Microsoft. Ze gebruiken veel technische termen om je ervan te overtuigen dat de problemen met jouw computer echt zijn. Ze kunnen je vragen enkele bestanden te openen of een scan op jouw computer uit te voeren - en je dan vertellen dat die bestanden of de scanresultaten een probleem laten zien... maar dat is er niet.

De oplichters kunnen dan:

Vragen hen op afstand toegang te geven tot jouw computer - waardoor zij toegang krijgen tot alle informatie die erop is opgeslagen en op elk netwerk dat ermee verbonden is malware installeren.

Toegang krijgen tot jouw computer en gevoelige gegevens, zoals gebruikersnamen en wachtwoorden kan downloaden.

Proberen je software of reparatiediensten te verkopen die waardeloos zijn of elders gratis verkrijgbaar zijn.

Proberen je in te schrijven voor een waardeloos computeronderhouds- of garantieprogramma

Vragen om creditcardgegevens zodat ze je een rekening kunnen sturen voor nepdiensten of diensten die elders gratis verkrijgbaar zijn

Je naar websites verwijzen en je vragen creditcard-, bankrekening- en andere persoonlijke gegevens in te voeren

MEER WETEN?
tiensecurity.nl

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

CYBERSECURITY VOOR
HET MKB

tien

HOE BESCHERM JE JOUW BEDRIJF

Als een beller zegt dat jouw computer een probleem heeft, hang dan op. Een technische ondersteuning die je niet verwacht is oplichterij - zelfs als het nummer lokaal is of legitiem lijkt. Deze oplichters gebruiken valse nummerinformatie om eruit te zien als lokale bedrijven of betrouwbare bedrijven.

Als je een pop-upbericht krijgt om technische ondersteuning te bellen, negeer deze dan. Sommige pop-upberichten over computerproblemen zijn legitiem, maar bel geen nummer of klik niet op een link die verschijnt in een pop-upbericht dat je waarschuwt voor een computerprobleem.

Als men zich zorgen maakt over een virus of een andere bedreiging, bel dan rechtstreeks met jouw beveiligingssoftwarebedrijf, via het telefoonnummer op de website, de kassabon of de verpakking van het product. Of raadpleeg onze expert.

Geef nooit iemand jouw wachtwoord, en geef geen toegang op afstand tot jouw computer aan iemand die onverwachts contact met je opneemt.

WAT DOE JE ALS JE BENT OPGELICHT

Als je jouw wachtwoord hebt gedeeld met een oplichter, verander het dan op elke account die dit wachtwoord gebruikt. Gebruik unieke wachtwoorden voor elke account en dienst. Overweeg het gebruik van een wachtwoordmanager.

Verwijder malware. Update of download legitieme beveiligingssoftware. Scan jouw computer en verwijder alles wat volgens de software een probleem is. Raadpleeg onze experts als je hulp nodig hebt.

Als de getroffen computer is aangesloten op uw netwerk, moet je of een beveiligingsdeskundige het hele netwerk controleren op inbraken.

Als je nepdiensten hebt gekocht, vraag jouw creditcardmaatschappij om de kosten terug te draaien en controleer uw afschrift op kosten die u niet heeft goedgekeurd. Blijf de creditcardafschriften controleren om er zeker van te zijn dat de oplichter je niet elke maand opnieuw probeert aan te rekenen.

MEER WETEN?
tiensecurity.nl

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

CYBERSECURITY VOOR
HET MKB

tien

CYBERVERZEKERING

Herstellen van een cyberaanval kan kostbaar zijn.

Een cyberverzekering is een optie die jouw bedrijf kan helpen beschermen tegen verliezen als gevolg van een cyberaanval. Als je een cyberverzekering overweegt, bespreek dan welke polis het beste past bij de behoeften van jouw bedrijf, inclusief of je moet kiezen voor een first-party dekking, een third-party dekking of beide. Hier zijn enkele algemene tips om te overwegen.

WAT ZOU JE CYBERVERZEKERING POLIS DEKKEN?

Zorg ervoor dat jouw polis dekking biedt voor:

- ☐ Datalekken (zoals incidenten met diefstal van persoonlijke informatie)
- ☐ Cyberaanvallen (zoals inbreuken op het netwerk)
- ☐ Cyberaanvallen op jouw gegevens in het bezit van verkopers en andere derden
- ☐ Cyberaanvallen die overal ter wereld plaatsvinden (niet alleen in Europa)
- ☐ Terroristische aanslagen

Overweeg ook of jouw cyberverzekeraar dat doet:

- ☐ Je verdedigen in een rechtszaak of een regelgevend onderzoek
- ☐ Dekking bieden boven alle andere toepasselijke verzekeringen die je hebt
- ☐ Een hotline voor problemen aanbieden die elke dag van het jaar op elk moment beschikbaar is

MEER WETEN?
tiensecurity.nl

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

CYBERSECURITY VOOR
HET MKB

tien

WAT IS
FIRST-PARTY DEKKING
EN WAAR MOET JE NAAR KIJKEN?

First-party (eigen schade) cyberdekking beschermt jouw gegevens, inclusief informatie over werknemers en klanten. Deze dekking omvat doorgaans de kosten van jouw bedrijf in verband met:

- ☐ Juridisch advies om de verplichtingen inzake kennisgeving en regelgeving te bepalen
- ☐ Kennisgeving aan klanten en callcenterdiensten Verloren inkomsten
- ☐ Crisisbeheer en public relations
- ☐ Forensische diensten om de inbreuk te onderzoeken
- ☐ Herstel en vervanging van verloren of gestolen gegevens
- ☐ Door bedrijfsonderbreking
- ☐ Cyberafpersing en -fraude
- ☐ Vergoedingen, boetes en sancties in verband met het cyberincident

WAT IS
THIRD-PARTY DEKKING
EN WAAR MOET JE NAAR KIJKEN?

Third-party cyberdekking (aansprakelijkheidsverzekering) beschermt je over het algemeen tegen aansprakelijkheid als een derde partij vorderingen tegen je instelt. Deze dekking omvat doorgaans:

- ☐ Betalingen aan door de inbreuk getroffen consumenten
- ☐ Claims en schikkingskosten in verband met geschillen of rechtszaken
- ☐ Verliezen in verband met laster en inbreuk op het auteursrecht of handelsmerk schending
- ☐ Kosten voor rechtszaken en het reageren op onderzoeken van regelgevende instanties
- ☐ Andere schikkingen, schadevergoedingen en vonnissen
- ☐ Boekhoudkundige kosten

MEER WETEN?
tiensecurity.nl

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

CYBERSECURITY VOOR
HET MKB

tien

EMAIL AUTHENTICATIE

Technologie voor e-mailverificatie maakt het een stuk moeilijker voor een oplichter om phishing e-mails te sturen die eruit zien alsof ze van jouw bedrijf afkomstig zijn.

Het gebruik van technologie voor e-mailverificatie maakt het voor oplichters veel moeilijker om phishing-e-mails te versturen. Met deze technologie kan een ontvangende server een e-mail van jouw bedrijf verifiëren en e-mails van een bedrieger blokkeren - of ze naar een quarantainemap sturen en je er vervolgens over informeren.

WAT MOET JE WETEN

Bij sommige providers van webhosting kan je de zakelijke e-mail van jouw bedrijf instellen met jouw domeinnaam (die je misschien beschouwt als de websitenaam). Jouw domeinnaam kan er zo uitzien: jouwbedrijf.nl. En jouw e-mail kan er zo uitzien: naam@jouwbedrijf.nl. Zonder e-mailverificatie kunnen scammers dat domeinnaam gebruiken om e-mails te versturen die eruitzien alsof ze van jouw bedrijf afkomstig zijn. Als jouw zakelijke e-mail de domeinnaam van jouw bedrijf gebruikt, zorg er dan voor dat de e-mailprovider over deze drie hulpmiddelen voor e-mailverificatie beschikt:

Sender Policy Framework (SPF)

vertelt andere servers welke servers e-mails mogen versturen met de domeinnaam van uw bedrijf. Dus wanneer u een e-mail stuurt vanaf naam@jouwbedrijf.nl, kan de ontvangende server bevestigen dat de verzendende server op een goedgekeurde lijst staat. Als dat zo is, laat de ontvangende server de e-mail door. Als er geen overeenkomst wordt gevonden, kan de e-mail als verdacht worden gemarkeerd.

Domain Keys Identified Mail (DKIM)

zet een digitale handtekening op uitgaande e-mail, zodat servers kunnen controleren of een e-mail van jouw domein daadwerkelijk vanaf de servers van jouw organisatie is verzonden en er tijdens het vervoer niet mee is geknoeid.

Domain-based Message Authentication, Reporting & Conformance (DMARC)

is het essentiële derde hulpmiddel voor e-mailverificatie. SPF en DKIM verifiëren het adres dat de server "achter de schermen" gebruikt. DMARC controleert of dit adres overeenkomt met het "van"-adres dat u ziet. Hiermee kan je ook andere servers vertellen wat ze moeten doen als ze een e-mail krijgen die van jouw domein afkomstig lijkt te zijn, maar de ontvangende server reden heeft om argwaan te hebben (gebaseerd op SPF of DKIM). Je kan andere servers de e-mail laten weigeren, als spam laten markeren of geen actie laten ondernemen. Je kan ook DMARC instellen zodat je op de hoogte wordt gebracht wanneer dit gebeurt.

MEER WETEN?
tiensecurity.nl

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

CYBERSECURITY VOOR
HET MKB

tien

WAT MOET JE DOEN ALS JE

EMAIL IS GESPOOFT

E-mailverificatie helpt voorkomen dat de e-mail van het bedrijf wordt gebruikt in phishingconstructies, omdat het je waarschuwt als iemand de e-mail van jouw bedrijf vervalst. Als je die melding krijgt, onderneem dan de volgende acties:

Meld het

Meld het bij de politie. Je kan phishing-e-mails ook doorsturen naar reportphishing@apwg.org (een adres dat wordt gebruikt door de Anti-Phishing Working Group, waarin ISP's, beveiligingsleveranciers, financiële instellingen en wetshandhavingsinstanties zijn vertegenwoordigd).

Bericht je klanten

Als je ontdekt dat scammers zich voordoen als jouw bedrijf, vertel dit dan zo snel mogelijk aan jouw klanten - per post, e-mail of sociale media. Als je jouw klanten een e-mail stuurt, stuur dan een e-mail zonder hyperlinks: je wilt niet dat jouw kennisgevingsmail lijkt op een phishing-scam. Herinner klanten eraan geen persoonlijke informatie te delen via e-mail of sms.

Waarschuw je collega's

Gebruik deze ervaring om de beveiligingspraktijken bij te werken en jouw personeel op te leiden over cyberdreigingen.

MEER WETEN?
tiensecurity.nl

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

CYBERSECURITY VOOR
HET MKB

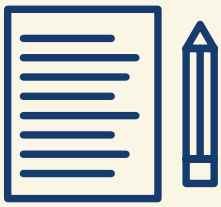
tien

VENDOR SECURITY

Uw zakelijke vendoren kunnen toegang hebben tot gevoelige informatie.

Probeer vast te stellen of leveranciers hun eigen computers en netwerken beveiligen. Wat als bijvoorbeeld jouw accountant, die over alle financiële gegevens beschikt, zijn laptop verliest? Of als een leverancier wiens netwerk verbonden is met dat van jou wordt gehackt? Het resultaat: jouw bedrijfsgegevens en de persoonlijke gegevens van jouw klanten kunnen in verkeerde handen vallen - waardoor jouw bedrijf en jouw klanten gevaar lopen.

HOE MONITOR JE DE LEVERANCIERS



Schrijf het op

Neem bepalingen op in de leverancierscontracten, zoals een plan voor het evalueren en bijwerken van beveiligingscontroles, aangezien bedreigingen veranderen. Maak de bepalingen die voor jouw bedrijf van cruciaal belang zijn niet-onderhandelbaar.

Check compliancy

Stel processen vast zodat je kunt bevestigen dat verkopers de regels volgen. Geloof ze niet zomaar op hun woord.

Maak aanpassingen

Cyberbeveiligingsbedreigingen veranderen snel. Zorg ervoor dat jouw leveranciers hun beveiliging up-to-date houden.

MEER WETEN?
tiensecurity.nl

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

CYBERSECURITY VOOR
HET MKB

tien

HOE BESCHERM JE JOUW BEDRIJF

Toegangscontrole

Zet controles op databases met gevoelige informatie. Beperk de toegang tot een "need-to-know" basis, en alleen voor de tijd die een verkoper nodig heeft om zijn werk te doen.

Gebruik multi-factor authenticatie

Hierdoor moeten vendoren naast het inloggen met een wachtwoord extra stappen nemen om toegang te krijgen tot jouw netwerk - zoals een tijdelijke code op een smartphone of een sleutel die in een computer wordt gestoken.

Beveilig je netwerk

Eis sterke wachtwoorden: minstens 12 tekens met een mix van cijfers, symbolen en hoofdletters en kleine letters. Gebruik wachtwoorden nooit opnieuw, deel ze niet, en beperk het aantal mislukte inlogpogingen om aanvallen met een wachtwoord te beperken.

Bescherm de gegevens

Gebruik goed geconfigureerde, sterke encryptie. Dit beschermt gevoelige informatie bij overdracht en opslag.

WAT TE DOEN ALS EEN VENDOR EEN DATALEK HEEFT

Bel de politie

Meld de aanval meteen bij de politie. Als zij niet bekend zijn met het onderzoeken van informatie-inbreuken, neem dan contact op onze experts.

Bevestig dat de vendor een oplossing heeft

Zorg ervoor dat de leverancier de kwetsbaarheden verhelpt en ervoor zorgt dat jouw informatie veilig blijft, als je bedrijf besluit de leverancier te blijven gebruiken.

Bericht klanten

Als jouw gegevens of persoonlijke informatie zijn gestolen, zorg er dan voor dat je de getroffen partijen op de hoogte brengt - zij kunnen het risico lopen op identiteitsdiefstal. Informatie over hoe je dat moet doen vind je op Data Breach Response: Een gids voor bedrijven.

MEER WETEN?
tiensecurity.nl

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

CYBERSECURITY VOOR
HET MKB

tien

HOSTING KIEZEN

Misschien wil je een nieuwe of verbeterde website voor jouw bedrijf.

Maar als je niet over de vaardigheden beschikt om het web op te zetten dat jij wilt, wil je misschien een provider van webhosting inhuren om het voor je te doen. Of je nu een website upgradet of een nieuw bedrijf lanceert, er zijn veel opties voor webhosting. Bij het vergelijken van diensten moet veiligheid een belangrijk aandachtspunt zijn.

WAAR NAAR TE KIJKEN

Transport Layer Security (TLS)

De dienst die u kiest moet TLS bevatten, wat de privacy van jouw klanten helpt beschermen. (Je hebt misschien al gehoord van zijn voorganger, Secure Sockets Layer, of SSL.)

TLS zorgt ervoor dat uw klanten op uw echte website terechtkomen wanneer zij uw URL in de adresbalk typen. Wanneer TLS correct is geïmplementeerd op uw website, begint jouw URL met https://.

TLS zorgt er ook voor dat de informatie die naar jouw website wordt gestuurd, wordt versleuteld. Dat is vooral belangrijk als je klanten om gevoelige informatie vraagt, zoals creditcardnummers of wachtwoorden.

E-mail verificatie

Bij sommige providers van webhosting kan je de zakelijke e-mail van jouw bedrijf instellen met jouw domeinnaam (dat is een deel van de URL, en wat je misschien ziet als uw websitenaam). Jouw domeinnaam kan er zo uitzien: jouwbedrijf.nl. En jouw e-mail kan er zo uitzien: naam@jouwbedrijfs.nl. Als je geen e-mailverificatie hebt, kunnen scammers zich voordoen als die domeinnaam en e-mails sturen die van jouw bedrijf afkomstig lijken te zijn. Wanneer jouw zakelijke e-mail is ingesteld met de domeinnaam van jouw bedrijf, zorg er dan voor dat jouw webhost ujedeze drie hulpmiddelen voor e-mailverificatie kan bieden:

- Sender Policy Framework (SPF)
- Domain Keys Identified Mail (DKIM)
- Domain-based Message Authentication, Reporting & Conformance (DMARC)

MEER WETEN?
tiensecurity.nl

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

CYBERSECURITY VOOR
HET MKB

tien

WAAR NAAR TE KIJKEN

Software updates

Veel aanbieders van webhosting bieden kant-en-klare websites of pakketten die ontworpen zijn om de website van jouw bedrijf snel en gemakkelijk op te zetten. Zoals bij alle software is het essentieel dat je de nieuwste versies gebruikt met actuele beveiligingspatches. Zorg ervoor dat je weet hoe je de software van de website up-to-date houdt, of dat de webhostprovider dit voor je doet.

Website management

Als een webhostprovider jouw website beheert, moet je mogelijk via die provider wijzigingen aanbrengen - hoewel je misschien zelf kunt inloggen en enkele wijzigingen kunt aanbrengen. Sommige aanbieders van webhosting bieden in plaats daarvan de mogelijkheid om de website zelf te beheren. Het is belangrijk om vanaf het begin duidelijk te maken wie de website zal beheren nadat deze is gebouwd.

WAT MOET JE VRAGEN

Wanneer je een webhostprovider inhuurt, stel dan deze vragen om er zeker van te zijn dat je jouw klanteninformatie en jouw bedrijfsgegevens helpt beschermen.

- ☐ Is TLS inbegrepen in het hosting pakket? betaalde add-on? Stel ik het zelf in of helpen jullie me bij het inrichten?
- ☐ Kan mijn zakelijke e-mail mijn zakelijke websitenaam gebruiken? Zo ja, kan je mij helpen met het opzetten van SPF, DKIM, en DMARC e-mail authenticatie technologie? (Zo nee, overweeg dan een provider te zoeken die dat wel kan).
- ☐ Zijn de meest actuele softwareversies beschikbaar bij de dienst, en houd je de software up-to-date? Als het mijn verantwoordelijkheid is om software up-to-date te houden, is dat dan gemakkelijk voor mij?
- ☐ Nadat de website is opgezet, wie kan er dan wijzigingen aanbrengen? Moet ik dat via jullie doen? Kan ik zelf inloggen en wijzigingen aanbrengen? Als ik kan inloggen om wijzigingen aan te brengen, is multi-factor authenticatie beschikbaar?

MEER WETEN?
tiensecurity.nl

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

CYBERSECURITY VOOR
HET MKB

tien

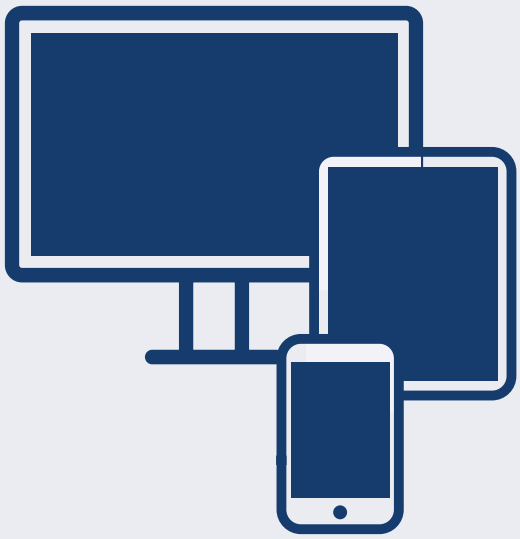
VEILIGE TOEGANG OP AFSTAND

Werknemers en leveranciers moeten wellicht op afstand verbinding maken met jouw netwerk.

Zet de beveiliging van jouw netwerk op de eerste plaats. Zorg ervoor dat werknemers en leveranciers strenge beveiligingsnormen volgen voordat ze verbinding maken met jouw netwerk. Geef ze de middelen om beveiliging onderdeel van hun werkroutine te maken.

HOE JE
DEVICES TE BESCHERMEN

Of werknemers of leveranciers nu door het bedrijf verstrekte apparaten of hun eigen apparaten gebruiken om op afstand verbinding te maken met uw netwerk, deze apparaten moeten veilig zijn. Volg deze tips - en zorg ervoor dat uw werknemers en leveranciers dat ook doen:



Wijzig altijd vooraf ingestelde routerwachtwoorden en de standaardnaam van de router. En houd de software van de router software up-to-date.

Overweeg volledige schijfversleuteling in te schakelen voor laptops en andere mobiele apparaten die op afstand verbinding maken met het netwerk. Controleer of het besturingssysteem deze optie biedt, die alle gegevens op het apparaat beschermt als het zoekraakt of wordt gestolen. Dit is vooral belangrijk als het apparaat gevoelige persoonlijke informatie bevat.

Wijzig de instellingen van de smartphone om automatische verbindingen met openbare Wi-Fi te stoppen.

Zorg voor up-to-date antivirussoftware op apparaten die verbinding maken met jouw netwerk, inclusief mobiele apparaten.

MEER WETEN?
tiensecurity.nl

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

CYBERSECURITY VOOR

HET MKB

tien

HOE TE VERBINDEN MET JE NETWERK OP AFSTAND

Eis van werknemers en verkopers dat zij veilige verbindingen gebruiken wanneer zij op afstand verbinding maken met uw netwerk. Ze moeten:

Gebruik een router met WPA2- of WPA3-encryptie wanneer zij thuis verbinding maken. Encryptie beschermt informatie die via een netwerk wordt verzonden, zodat buitenstaanders deze niet kunnen lezen. WPA2 en WPA3 zijn de enige versleutelings-normen die de via een draadloos netwerk verzonden informatie beschermen.

Gebruik alleen openbare Wi-Fi als je ook een virtueel privénetwerk (VPN) gebruikt om het verkeer tussen uw computer en het internet te versleutelen. Openbare Wi-Fi biedt op zichzelf geen veilige internetverbinding. Jouw werknemers kunnen een persoonlijk VPN-account krijgen van een VPN-dienstverlener, of kunt een leverancier inhuren om een bedrijfs-VPN te maken voor alle werknemers.

HOE BEHOUD JE DE CYBERSECURITY

Train je collega's:

Informatie over veilige toegang op afstand opnemen in regelmatige opleidingen en in de oriëntatie van nieuw personeel.

Zorg voor een beleid voor elementaire cyberbeveiliging, geef kopieën aan jouw werknemers en leg uit hoe belangrijk het is om dit beleid te volgen.

Voordat je een apparaat - bij een werknemer thuis of op het netwerk van een leverancier - verbinding laat maken met jouw netwerk, moet je ervoor zorgen dat het voldoet aan de beveiligingsvereisten van jouw netwerk.

Vertel je personeel over de risico's van openbare Wi-Fi.

Geef jouw personeel hulpmiddelen om de veiligheid te handhaven:

- Eis van werknemers dat zij unieke, complexe netwerkwachtwoorden gebruiken en vermijd onbeheerde, open werkstations.
- Eis multi-factor authenticatie voor toegang tot delen van het netwerk met gevoelige informatie. Dit vereist extra stappen naast het inloggen met een wachtwoord - zoals een tijdelijke code op een smartphone of een sleutel die in een computer wordt gestoken.
- Overweeg een VPN die werknemers kunnen gebruiken wanneer ze op afstand verbinding maken met het bedrijfsnetwerk.
- Als je op jouw bedrijfsterrein Wi-Fi aanbiedt voor gasten en klanten, zorg er dan voor dat dit gescheiden is van en niet verbonden is met jouw bedrijfsnetwerk.
- Neem beveiligingsbepalingen op in jouw leveranciers-contracten, vooral als de leverancier op afstand verbinding maakt met jouw netwerk.

MEER WETEN?
tiensecurity.nl

NIST
National Institute of Standards and Technology
U.S. Department of Commerce