advantive

CYBER SECURITY

Hoe ervoor zorgen dat jij en je collega’s alle data beter kunnen beveiligen?

INHOUDSOPGAVE

CYBER SECURITY

CYBER SECURITY

> Hoe kan je jezelf & anderen beschermen en voorkomen dat deze informatie in verkeerde handen valt?

Onze levens zijn meer en meer afhankelijk geworden van het internet. Het internet met al zijn gadgets en apparaten waar wij urenlang gebruik van maken, maken een groot deel van ons leven uit, ze zijn inmiddels diep in onze maatschappij geïntegreerd. Dit doen we zowel uit noodzaak omdat het verplicht wordt vanuit de overheid als ook omwille van het sociale leven.

Wil je je aansluiten bij een sportvereniging? Dan worden er basisgegevens opgeslagen in hun database. Ga je naar de dokter? Al je medische gegevens worden rechtstreeks in hun systeem ingegeven. Ga je online shoppen, dan moet je zeer gevoelige informatie doorgeven.

De maatschappij die reeds zeer gedigitaliseerd is, zal naar de toekomst toe alleen maar meer en meer afhankelijk worden van het internet. Hierdoor wordt het speelterrein van hackers steeds groter en groter waardoor Cyber Security ook steeds belangrijker en belangrijker zal worden.

CYBER SECURITY – WAT IS CYBER SECURITY?

Om te begrijpen waarom Cyber Security zo belangrijk is, starten we met Cyber Security uit te leggen. Cyber Security is het beschermen van elektronische informatie dat bewaard wordt in de virtuele wereld en de kwetsbaarheden die hierbij komen kijken zo veel mogelijk beperken.
Het belang van Cyber Security in de digitale wereld is enorm. Dit komt doordat de hoeveelheid en de complexiteit van cyber aanvallen als maar toenemen. Naarmate onze afhankelijk van technologie groeit, zal ook onze kwetsbaarheid voor deze aanvallen toenemen. Cyber Security helpt onze gegevens en systemen te beschermen tegen deze bedreiging.

CYBER SECURITY – HET BELANG ERVAN IN DE DIGITALE WERELD

Het belang van Cyber Security in de digitale wereld kan niet onderschat worden. Eén beveiligingslek kan grote gevolgen hebben in de onderling verbonden wereld van vandaag.
Misschien wel een van de meest bekende voorbeelden van een Cyber aanval met grote impact voor de betroffen personen is de aanval op het stroom net van Oekraïne waar meer dan 200 000 personen voor een aantal uren zonder stroom zaten. Dezelfde aanval had ook impact op verschillende Europese grote landen waaronder Frankrijk, Duitsland en Italië.

advantive

MEEST VOORKOMENDE CYBER AANVALLEN

MEEST VOORKOMENDE CYBER AANVALLEN

In de afgelopen jaren zijn er verschillende cyberaanvallen geweest die een verwoestende impact hebben gehad op bedrijven en individuen. Het gaat om diefstal van identiteitsgegevens, bankgegevens en het lekken van gevoelige gegevens. De belangrijkste reden hiervoor is dat de meeste mensen hun gegevens opslaan op cloudopslagdiensten zoals Dropbox of Google Drive. Deze aanvallen hebben het belang van sterke cyberbeveiligingsmaatregelen benadrukt. Zie hier enkele van de meest voorkomende cyberaanvallen.

CYBER AANVALLEN – PHISHING

Phishing is een type cyberaanval waarbij gebruikers worden misleid om op schadelijke koppelingen of bijlagen te klikken. Dit kan leiden tot diefstal van gevoelige informatie, zoals inloggegevens of financiële gegevens.

Terwijl de wereld volop inzet op technologische vooruitgang, blijven cybercriminelen uiteraard niet achter. Hieronder geef ik enkele voorbeelden van de nieuwste trends in de phishingwereld in 2023:

- **Phishing met behulp van Kunstmatige Intelligentie (AI):** Phishingaanvallers maken steeds vaker gebruik van kunstmatige intelligentie en machine learning om hun aanvallen realistischer en overtuigender te maken. Een voorbeeld hiervan is het gebruik van Google's AI Bard, waarmee je de AI kunt vragen om een e-mail te schrijven die perfect aansluit bij je doelwit.

- **Phishing via mobiele apps:** Mobiele gebruikers zijn een groeiend doelwit voor phishingaanvallen, aangezien steeds meer mensen vertrouwen hebben in de beveiliging van hun mobiele apparaten.

- **Phishing in verband met COVID-19:** De COVID-19-pandemie heeft geleid tot een toename van phishingaanvallen die inspelen op angst en onzekerheid over de pandemie. Voorbeelden hiervan zijn valse vaccinatie-e-mails of -berichten. Ondanks dat de pandemie minder in het nieuws is, blijft het in 2023 een actueel onderwerp.

- **Phishing op populaire platforms:** Phishers richten zich steeds vaker op populaire platforms zoals sociale media, cloudopslagdiensten en instant messaging-apps. Dit kan bijvoorbeeld gebeuren via berichten op Facebook met kwaadaardige links.

- **Verbeterde social engineering:** Phishingaanvallers ontwikkelen steeds verfijndere social engineering-vaardigheden en -technieken, waaronder het imiteren van bekende bedrijven of instanties om het vertrouwen van slachtoffers te winnen en hen te misleiden.

advantive

MEEST VOORKOMENDE CYBER AANVALLEN

CYBER AANVALLEN – MALWARE

Malware is een soort kwaadaardige software die computers en apparaten kan infecteren. Het kan informatie stelen, apparaten kapen of aanvallen uitvoeren op andere systemen.

CYBER AANVALLEN – DENIAL-OF-SERVICE

Een denial-of-service aanval is een type aanval waarbij gebruikers geen toegang krijgen tot een systeem of dienst. Dit kan gedaan worden door het systeem te overspoelen met verkeer of verzoeken of door het te beschadigen zodat het niet meer goed kan functioneren.

CYBER AANVALLEN – RANSOMWARE

Ransomware is malware die bestanden of systemen versleutelt en losgeld eist om ze te ontsleutelen. Het kan leiden tot het verlies van essentiële gegevens of de volledige uitschakeling van een systeem.

CYBER AANVALLEN – MAN-IN-THE-MIDDLE

Een MitM-aanval is een type aanval waarbij een aanvaller de communicatie tussen twee partijen onderschept. Dit kan gedaan worden door een netwerkverbinding af te luisteren of verkeer om te leiden naar een kwaadaardige server.

AANTAL & COMPLEXITEIT

HET AANTAL EN DE COMPLEXITEIT VAN CYBER AANVALLEN

Naarmate het aantal en de complexiteit van cyberaanvallen toeneemt, neemt ook het belang van Cyber Security toe. Cyber Security is essentieel omdat het organisaties en individuen helpt beschermen tegen cyberaanvallen. Cyber Security kan datalekken, identiteitsdiefstal en andere vormen van cybercriminaliteit helpen voorkomen. Organisaties moeten sterke cyberbeveiligingsmaatregelen nemen om hun gegevens en klanten te beschermen.

AANTAL & COMPLEXITEIT – TRANSFORMATIE NAAR DE CLOUD

De Cloud heeft ons denken over IT veranderd, maar heeft ook nieuwe beveiligingsrisico's geïntroduceerd. Een van de belangrijkste voordelen van de Cloud is dat het organisaties in staat stelt flexibeler te zijn en sneller te reageren op veranderingen. Deze flexibiliteit kan echter ook nieuwe beveiligingsrisico's met zich meebrengen. Een Cloud provider heeft bijvoorbeeld niet dezelfde beveiligingscontroles als een traditioneel datacenter op locatie.

AANTAL & COMPLEXITEIT – IMPACT OP DE BUSINESS

Het internet is voor de meeste bedrijven over de hele wereld een onmisbaar onderdeel geworden van de bedrijfsvoering. De toename van het internetgebruik heeft geleid tot een toename van cyberaanvallen, die een aanzienlijke impact kunnen hebben op de bedrijfsvoering. Cyber Security in bedrijven helpt om zich te beschermen tegen deze aanvallen, waaronder datalekken, phishing-zwendel en ransomware. Cyber Security kan bedrijven helpen om hun gegevens, klanten en reputatie te beschermen.

advantive

TIPS & TRICKS
EIGEN BESCHERMING

HOE KAN JE JOUW ORGANISATIE BESCHERMEN TEGEN CYBER CRIMINELEN?

Om je organisatie te beschermen tegen cybercriminaliteit moet je verschillende voorzorgsmaatregelen nemen. Ten eerste moet je een solide cyberbeveiligingsbeleid hebben. Dit beleid moet gegevensversleuteling, firewalls en inbraakdetectiesystemen omvatten.

1 Gegevensversleuteling

2 Firewalls

3 Inbraakdetectiesystemen

4 Trainen van werknemers tegen cyberbedreigingen

5 Constante check-up van het netwerk op verdachte activiteiten

Daarnaast moet u uw werknemers trainen om mogelijke cyberbedreigingen te herkennen en te melden.

Tot slot moet u uw netwerk regelmatig controleren op verdachte activiteiten. Als u deze stappen neemt, zult u de kans dat uw organisatie slachtoffer wordt van cybercriminaliteit aanzienlijk verkleinen.

advantive

TIPS & TRICKS
EIGEN BESCHERMING

HOE KUNNEN WERKNEMERS BETER WORDEN IN HET BEVEILIGEN VAN HUN DATA?

Er zijn veel redenen waarom mensen hun gegevens moeten beschermen. Eén reden is dat onbevoegden toegang kunnen krijgen tot gegevens en deze kunnen gebruiken als ze niet worden beschermd. Dit kan leiden tot identiteitsdiefstal, fraude en andere misdrijven. Zie hier enkele manieren waarop individuen hun gegevens beter kunnen beschermen.

TIPS & TRICKS – GEBRUIK STERKE WACHTWOORDEN

Indien je een wachtwoord moet gebruiken dan is het best dat deze minstens acht tekens is en een mix van hoofdletters en kleine letters, cijfers en symbolen bevat. Vermijd het gebruik van makkelijk te raden woorden zoals je naam of geboortedatum. De modernste systemen gebruiken zelfs geen wachtwoorden meer maar werken met biomedische informatie zoals je vingerafdruk of face ID.

TIPS & TRICKS – GEBRUIK EEN WACHTWOORDMANAGER

Een wachtwoordmanager is een applicatie die u kan helpen uw wachtwoorden bij te houden en sterke wachtwoorden te genereren.

TIPS & TRICKS – WACHTWOORDEN NIET HERGEBRUIKEN

Het hergebruiken van wachtwoorden maakt het hackers makkelijker om toegang te krijgen tot uw accounts.

TIPS & TRICKS – HOUD UW SOFTWARE UP-TO-DATE

Software-updates bevatten vaak beveiligingspatches die uw gegevens kunnen helpen beschermen.

TIPS & TRICKS – GEBRUIK MULTI FACTOR AUTHENTICATIE

Multi factor authenticatie voegt een extra beveiliging laag toe door je te vragen om naast je wachtwoord ook een code van je telefoon of e-mail in te voeren.

TIPS & TRICKS – WEES VOORZICHTIG MET PHISHING

Phishing is een e-mail of website die zich voordoet als een legitiem bedrijf om u te verleiden tot het invoeren van uw persoonlijke gegevens.

TIPS & TRICKS – MAAK REGELMATIG BACK-UPS VAN JE DATA

Een regelmatige back-up maken van je data zorgt ervoor dat je de zekerheid hebt terug aan alles te kunnen in het geval je laptop is gestolen of geblokkeerd. Behalve als je in de Cloud werkt, dan wordt dit meestal voor je gedaan.

ADVANTIVE

Get in touch with us on social media!

www.advantive.be

advantive

Adres

Thor Park 8300
3600 GENK

Contact

Telefoon: 089 39 59 19
E-mail: info@advantive.be