KNNS

Whitepaper

Doe de check

Is mijn cybersecurity goed geregeld?

Doe de check - is mijn cybersecurity goed geregeld?

Whitepaper

Cybersecurity uitgelegd

Het begrip cybersecurity hoor je de laatste tijd veel voorbij komen. Het betekent letterlijk ‘cyberbeveiliging’ waarin het woord ‘cyber’ alles omvat wat met technologie te maken heeft. Dus de beveiliging van je telefoon, laptop, IT-omgeving, je (persoonlijke) documenten, digitale bedrijfsgegevens, gegevens van klanten en zo gaat het lijstje door. Niet alleen binnen bedrijven leeft de term ‘cybersecurity’, ook bij onszelf als individu.

Sinds we steeds meer online voortbewegen, neemt de behoefte aan (online) privacy toe. Maar hoe zorgen we ervoor dat we veilig online zijn? En voor ondernemers: hoe weten we zeker dat ons bedrijfsnetwerk- en gegevens goed beveiligd zijn? Wat zijn mijn grootste risico’s? Onwetendheid is de allergrootste angst. En terecht, want niet alle cyberdreigingen of zelfs cyberaanvallen zijn direct zichtbaar. In deze whitepaper rekenen we af met die onwetendheid.

Whitepaper

Dit zijn de meest voorkomende cyberaanvallen

Malware

Malware is kwaadaardige software die wordt verspreid over je bedrijfsnetwerk/ werkplekken met als doel informatie te vergaren of toegang te krijgen tot je verschillende systemen. Er zijn verschillende soorten malware:

→ virussen (blokkeert je device doordat je een verkeerde download hebt gedaan),

ransomware (gijzelt bestanden door ze te versleutelen of jou buiten te sluiten van je eigen systeem),

→ trojans (software die zich verstopt heeft in andere software),

→ wormen (maakt misbruik van een lek in je systemen),

→ spyware (volgt waar je heen surft),

→ adware (publiceert ads op je scherm nadat je een verkeerd programma hebt geïnstalleerd) en

→ robots (dit zijn programma's die zichzelf verspreiden)

> De veiligheid van een IT infrastructuur vraagt om steeds meer aandacht. Daar zijn we ons meer dan ooit bewust van.
>
> Coert Tempelman

Phising

Hiermee wordt geprobeerd om via (persoonlijke) mail toegang te krijgen tot gevoelige gegevens of zelfs hele IT-omgevingen. De afzender van een phising mail lijkt vaak een bekende organisatie, maar als je beter kijkt naar bijvoorbeeld het e-mailadres of telefoonnummer dan zie je dat deze afwijkt en zelfs een beetje vreemd is. Meestal wordt er in een phising mail gevraagd om persoonlijke gegevens in te vullen zodat de persoon achter de mail (de dader) uiteindelijk toegang krijgt tot de gegevens waar hij naar op zoek was.

DDoS aanval

Met een DDoS (Distributed Denial of Service) aanval wordt je bedrijfsnetwerk, device of dienst zoals webshop overbelast waardoor deze niet meer toegankelijk is voor klanten of collega's.

Man-in-the-middle

Bij deze aanval staat er letterlijk één persoon in het midden tussen twee communicerende partijen waardoor deze het gesprek kan manipuleren of gevoelige informatie opvangt. Bijvoorbeeld: een organisatie stuurt een factuur naar een klant. De ‘man-in-the-middle’ (dader) onderschept deze mail en geeft er een eigen draai aan door het rekeningnummer op de factuur aan te passen naar zijn eigen rekeningnummer. De klant (het slachtoffer) maakt uiteindelijk het geld over naar de ‘man-in-the-middle’ en niet naar de organisatie waar de factuur in eerste instantie vandaan kwam. In de meeste gevallen komt het slachtoffer er pas achter wanneer het te laat is en het geld verdwenen is.

SQL-injectie

Bij een SQL-injectie gebruikt een hacker een codefragment om op een manipulatieve manier toegang te krijgen tot een database met waardevolle informatie.

Zero day exploit

Zero day betekent ‘dag 0’. Deze vorm van cyberaanval richt zich op de nog onontdekte kwetsbaarheden van net gelanceerde, nieuwe software.

Brute force attack

Bij deze aanval probeert de hacker zoveel mogelijk inlognamen in combinatie met wachtwoorden uit totdat deze de juiste heeft gevonden en kan inloggen. Te makkelijke wachtwoorden of onveilig opgeslagen wachtwoorden zijn hierin een zwakke plek.

Cross-site scripting

Cross-site scripting richt zich op de eindgebruiker. Aanvallers injecteren kwade scripts in websites en applicaties met als doel het apparaat van de eindgebruiker te bemachtigen om bijvoorbeeld inzicht te krijgen in bankgegevens, social media of andere websites. Dit is vaak geen persoonlijke aanval, maar heeft de eindgebruiker gewoon pech dat hij of zij het doelwit is geworden. Hoewel dit geen aanval op jouw bedrijf is, kan het funest zijn voor je bedrijfsimago.

Rootkits

Een rootkit is een aanval waarbij het zichzelf, of andere malware verstopt. Daardoor wordt deze vaak niet ontdekt door anti-malwaresoftware. Met een rootkit willen hackers toegang krijgen tot het bedrijfsnetwerk of de devices en blijven daar ook onopgemerkt hangen.

IoT-aanval

Door IoT (Internet of Things) zijn er heel veel online apparaten bijgekomen. Denk aan auto’s, lichtbronnen, ijskast, apparatuur voor netwerkopslag (NAS) en horloges. Beveiliging van deze apparaten staat bij de producenten vaak niet bovenaan de to-do-lijst waardoor deze voor hackers makkelijker binnen te dringen zijn. Zo kan het hacken van de bedrijfsauto zo maar eens leiden tot het binnendringen van hackers in jouw online omgeving.

Feit of fabel: de grootste cyberrisico’s komen van binnenuit je organisatie

Goede cybersecurity valt of staat niet alleen in het goed beveiligen van je IT-omgeving door bijvoorbeeld het plaatsen een firewall, het up-to-date houden van je devices of het installeren van anti-virussoftware. Natuurlijk ontstaan er risico’s door gebreken in de techniek, maar het (onbewuste) gedrag van medewerkers vormt veruit het grootste risico. Niemand, maar dan ook écht niemand binnen een organisatie heeft inzicht in wanneer collega X van afdeling finance op een phising mail heeft geklikt of een verkeerde download heeft gedaan. En niemand heeft door dat medewerker Y op vakantie verbinding heeft gemaakt met een openbaar Wi-Fi netwerk. waardoor er nu deeltjes malware via je IT-omgeving verspreid worden of gevoelige gegevens worden achterhaald. Je merkt dit helaas pas op als het te laat is. Als er bijvoorbeeld een onbekende rekeninghouder geld afschrijft van je rekening. Of wanneer je wordt geconfronteerd met je eigen gestolen gegevens.

We zien dit door het ontbreken van een duidelijke visie en beveiligingsbeleid vaak misgaan. In het beveiligingsbeleid staat bijvoorbeeld wie welke admin rechten heeft, welke overbodige functies kunnen worden uitgeschakeld, wanneer updates uitgevoerd moeten worden en welke anti-virus software geïnstalleerd dient te zijn.

> Het is dus een feit: de grootste cybersecurity risico’s ontstaan binnen eigen kantoormuren.

De gevolgen van slechte cybersecurity

Dreigingen in cybersecurity zijn geen ver van je bedshow meer en steeds vaker zijn bedrijven slachtoffer van een cyberaanval. De gevolgen van een cyberaanval brengen altijd kosten en/of schade met zich mee. De meest voorkomende gevolgen zijn:

Diefstal van gegevens

Met een slinkse cyberaanval kunnen gegevens gestolen worden door hackers. Ze kunnen deze vervolgens doorverkopen aan concurrenten of vernietigen. Of je krijgt je eigen gegevens terug aangeboden, maar dan hangt daar wel een flink prijskaartje aan.

Je website is niet meer bereikbaar

Wanneer je website wordt platgelegd kunnen huidige of potentiële klanten je niet meer bereiken. Of er kunnen geen nieuwe orders meer geplaatst worden. Hierdoor loop je mogelijk omzet mis. Hoe langer je website niet bereikbaar is, hoe slechter het is voor je reputatie en hoe meer omzet je misloopt.

Imagoschade

Klantdata die op straat is komen te liggen, of gevoelige bedrijfsinformatie die wordt gepubliceerd waarvan je liever niet had dat die gedeeld werd. Dit kan er allemaal voor zorgen dat de reputatie van jouw organisatie ten onder gaat. Een imago verbeteren kost heel veel tijd, geld en energie en kan best lastig of zelfs onmogelijk zijn. Daarnaast kan zelfs het feit dat je überhaupt slachtoffer bent geworden van cybercriminaliteit, zorgen voor verlies van vertrouwen en een slecht imago.

Faillissement

Cybercriminelen vragen zonder pardon om enorme bedragen voor het teruggeven van gegevens of herstellen van geblokkeerde systemen. Daar heb je natuurlijk niet op gerekend. In sommige gevallen lukt het niet om deze te betalen waardoor er niks anders meer op zit dan uiteindelijk een faillissement aan te vragen. Of het imago van jouw bedrijf heeft zo'n grote schade opgelopen dat deze niet meer te herstellen is, door het verlies van alle bedrijfsgegevens en klantdata waardoor het 'gewoon doorgaan' ook geen optie meer is.

Ben ik al cyberslachtoffer?

Een van de grootste onzekerheden van directie en managementteam is het huidige niveau van cybersecurity. Gezien verantwoordelijkheid die je in deze functie draagt, wil je graag kennis hebben van het niveau waar je nu staat met cybersecurity en hoe dit geregeld is. Maar eigenlijk weet je niet precies hoe de vork in de steel steekt. Misschien komt dat doordat jouw technische kennis ontbreekt of de eigen IT-afdeling moeite heeft met het overbrengen van de ins- en outs met betrekking tot security. Dat laatste is niet raar, want cybersecurity is nou eenmaal veelomvattend en specialistisch werk.

Helaas is het niet mogelijk om met terugwerkende kracht na te gaan of je al slachtoffer bent (geweest) van cybercriminaliteit. Wel kunnen we, aan de hand van een ‘proof of concept’, een maand lang jouw bedrijfsnetwerk op cybersecurity monitoren vanuit het Security Operating Centre. Hier zit een team van specialisten met ervaring in cyberdreiging en -aanvallen. Zij merken verdachte activiteiten op en kunnen aan de hand daarvan een inschatting maken van het huidige niveau van cybersecurity. Hiermee kan jij zelf of met onze hulp aan de slag de beveiliging van jouw organisatie te verbeteren.

Checklist voor een goede cybersecurity

Je hebt een security beleid opgesteld

In het security beleid wordt het doel, de richting, de principes en de basisregels voor informatiebeveiliging geformuleerd.

Je hebt alle processen en bedrijfsrisico’s inzichtelijk

Hierdoor weet je waar de belangrijkste aandachtspunten voor cybersecurity liggen. Daarnaast zorgt inzicht in processen zoals toegangsrechten, fysieke beveiliging en beveiliging in bedrijfsvoering ervoor dat je het security beleid ook daadwerkelijk kan realiseren.

Je hebt een helder inzicht in het huidige niveau van cybersecurity

Het is belangrijk dat je weet wat je huidige niveau van cybersecurity is. Enerzijds om te weten wat de risico’s zijn, en anderzijds om op een later moment te kunnen toetsen of je cybersecurity verbeterd is.

Je hebt regels en maatregelen ingesteld die betrekking hebben op: hardening, security patches, anti-virus, vulnerabilities en autorisaties

Er zijn een aantal technische basismaatregelen die je kan nemen om cybersecurity te verbeteren. Deze zijn opgesteld door het CIS (Centre for Internet Security) en ze maken onderdeel uit van maatregelen die betrekking hebben op de AVG. Onderzoek heeft aangetoond dat invoering van de maatregelen effectieve bescherming biedt tegen ongeveer 85% van de meest gebruikelijke cyberaanvallen.

Whitepaper

Je hebt een slim digitaal immuunsysteem geïmplementeerd

Het digitale immuunsysteem voor organisaties leert wat ‘normale patronen’ zijn om zo nog onbekende cyberdreiging te herkennen. Het systeem beschermt de hele digitale onderneming waaronder de Cloud, gevirtualiseerde omgevingen, SaaS-applicaties en industriële controlesystemen.

Voor productieorganisaties beschermt het immuunsysteem naast de digitale onderneming (IT), ook het hele digitale productieproces. Het dure woord hiervoor is Operational Technology (OT). Ondersteund door een aantal “key” technologieën vormt het digitale immuunsysteem een heel belangrijke factor

Periodiek deelt jouw IT-afdeling de rapportages die betrekking hebben op cybersecurity

Cybersecurity goed regelen is één. Monitoring ervan is minstens net zo belangrijk. De regels en maatregelen die zijn ingesteld, moeten in de gaten gehouden worden. Dit geldt ook voor het digitale immuunsysteem dat is geïmplementeerd. Hierdoor weet je waar je nog kan verbeteren en inzien welke dreigingen zich de afgelopen periode hebben voorgedaan.

Stop nooit met verbeteren

Cybersecurity is nooit voldoende. Hackers worden steeds slimmer en de aanvallen zijn steeds moeilijker te herkennen. Daarom is het goed om altijd inzicht te houden in waar jouw organisatie staat op het gebied van cybersecurity en waar je nog kan verbeteren. Voor een ISO 27001-certificering is dit sowieso een vereiste. Zorg er tot slot voor dat je in bezit bent van de juiste tools om rapportages te kunnen draaien en maak medewerkers bewust van alle gevaren. Een beetje cliché maar ook hier geldt: voorkomen is altijd beter dan genezen.

Whitepaper

KNNS

Hulp nodig bij het goed regelen van cybersecurity?

Altijd vooruit denken. Altijd excelleren. Dat is KNNS. Waar wij het verschil maken? Vanuit een uitgekiende strategie ligt onze volledige focus op de digitale gezondheid en veiligheid van jouw organisatie. Zodat jij klaar bent voor elke uitdaging van morgen. Meer weten?

Neem contact op met Marcel voor advies

088 - 5667 000

m.schraven@knns.nl