niceCloud

CHECKLIST CYBERSECURITY

> ***Geen marketingpraat, maar een eerlijke analyse van jouw cybersecurity, zodat je grip houdt op risico's.***
>
> - IT-manager productiebedrijf

Cyberdreigingen wachten niet. Ontdek vandaag hoe weerbaar jouw organisatie écht is.

NiceCloud. Deskundig geregeld. Met plezier gedaan.

VOORWOORD

Cybersecurity staat bij vrijwel iedere organisatie op de agenda. Toch zien we in de praktijk dat het vaak pas echt aandacht krijgt nadat er iets misgaat.

Niet omdat IT-managers of directies het belang niet inzien, maar omdat het lastig is om objectief te bepalen waar je staat. Wat is goed geregeld, wat niet, en waar loop je ongemerkt risico?

Bij NiceCloud werken we dagelijks met organisaties die grip willen houden op hun IT-omgeving. Wat daarbij steeds terugkomt, is de behoefte aan rust, overzicht en voorspelbaarheid. Cybersecurity moet helpen om die rust te creëren, niet om extra stress toe te voegen.

Deze checklist is bedoeld als hulpmiddel. Geen audit, geen verkoopverhaal, maar een eerlijke spiegel. Zodat je zelf kunt beoordelen of je cybersecurity op hoofdlijnen op orde is, of dat het tijd is om scherper te kijken.

Johan Land
Managing partner

ZO GEBRUIK JE DE CHECKLIST

Deze checklist helpt je om in korte tijd inzicht te krijgen in de staat van je cybersecurity.

Beantwoord elke vraag met **JA** of **NEE**.

Twijfel je over een antwoord? Zie dat als een aandachtspunt. Elke “NEE” of twijfel is een signaal dat extra aandacht nodig is.

De checklist is bewust praktisch gehouden. Niet technisch diepgaand, maar wel scherp genoeg om risico’s zichtbaar te maken.

Het doel is bewustwording en richting, niet beoordelen.

niceCloud

NiceCloud. Deskundig geregeld. Met plezier gedaan.

1. BELEID EN VERANTWOORDELIJKHEID

Ja / Nee	**Is er een actueel, schriftelijk cybersecuritybeleid?**
Ja / Nee	**Is duidelijk wie binnen de organisatie eindverantwoordelijk is voor cybersecurity?**
Ja / Nee	**Wordt het beleid minimaal jaarlijks geëvalueerd en aangepast?**

Notities:

In veel organisaties bestaat securitybeleid wel, maar leeft het nauwelijks. Het is vaak ooit opgesteld, maar niet actief bijgewerkt of besproken. Zonder duidelijke eigenaar blijft cybersecurity versnipperd en vooral reactief.

2. TOEGANGSBEHEER EN BACK-UP (1)

Toegangsbeheer en accounts

Ja / Nee	**Is multi-factor authenticatie verplicht voor alle accounts?**
Ja / Nee	**Voldoen wachtwoorden aan sterke eisen en worden ze periodiek vernieuwd?**
Ja / Nee	**Worden accounts van vertrokken medewerkers direct afgesloten?**
Ja / Nee	**Is er een actueel overzicht van alle gebruikers en rechten?**

Notities:

Toegangsrechten groeien vaak mee met functies, maar krimpen zelden mee. Daardoor blijven rechten bestaan die niet meer nodig zijn. Dit risico blijft meestal onzichtbaar tot het moment dat er misbruik van wordt gemaakt.

2. TOEGANGSBEHEER EN BACK-UP (2)

Back-up en herstel

Ja / Nee	**Worden dagelijks automatische back-ups gemaakt van kritieke data?**
Ja / Nee	**Zijn back-ups extern en versleuteld opgeslagen?**
Ja / Nee	**Is minimaal één keer per jaar getest of herstel werkt?**
Ja / Nee	**Is er een actueel disaster recovery plan?**

Notities:

Back-ups geven een gevoel van zekerheid, maar die zekerheid is pas echt als herstel getest is. In de praktijk blijkt regelmatig dat data wel is opgeslagen, maar niet volledig of niet tijdig kan worden teruggezet.

3. UPDATES EN MONITORING

Updates en patchmanagement

Ja / Nee	**Worden systemen en applicaties tijdig geüpdatet?**
Ja / Nee	**Is er inzicht in gebruikte software en update-status?**
Ja / Nee	**Worden kwetsbaarheden actief opgevolgd?**

Monitoring en detectie

Ja / Nee	**Is er 24/7 monitoring op verdachte activiteiten?**
Ja / Nee	**Worden incidenten automatisch gemeld?**
Ja / Nee	**Is inzichtelijk wie wanneer toegang heeft tot kritieke systemen?**

Notities:

Updates worden vaak uitgesteld om verstoring te voorkomen. Tegelijkertijd blijven kwetsbaarheden zo langer openstaan. Zonder actieve monitoring blijft afwijkend gedrag onopgemerkt en wordt een incident vaak pas ontdekt wanneer de impact al groter is.

4. AWARENESS EN COMPLIANCE

Awareness en training

Ja / Nee	**Volgen medewerkers jaarlijks een security awareness-training?**
Ja / Nee	**Worden phishing-simulaties uitgevoerd?**
Ja / Nee	**Is er een meldpunt voor verdachte e-mails?**

Compliance en audits

Ja / Nee	**Kun je aantonen dat je voldoet aan AVG, NIS2 en relevante normen?**
Ja / Nee	**Worden periodiek audits uitgevoerd?**
Ja / Nee	**Is duidelijk welke eisen voor jouw organisatie gelden?**

Notities:

Medewerkers vormen geen zwakke schakel uit onwil, maar door gebrek aan context. Zonder training is het lastig om phishing of social engineering te herkennen. Compliance wordt daarbij vaak gezien als een vinkje, terwijl het in de praktijk draait om dagelijks gedrag en werkprocessen.

5. INCIDENT RESPONSE EN CLOUD

Incident response en crisismanagement

Ja / Nee	**Is er een actueel incident response plan?**
Ja / Nee	**Weet iedereen wat te doen bij een cyberincident?**
Ja / Nee	**Is het plan geoefend en geëvalueerd?**

Cloud en shadow IT

Ja / Nee	**Is er inzicht in alle gebruikte cloud- en SaaS-applicaties?**
Ja / Nee	**Is duidelijk wie verantwoordelijk is voor cloud security?**

Notities:

Veel organisaties hebben wel een incidentplan, maar hebben het nooit geoefend. In een stressvolle situatie blijkt dan dat rollen en stappen onduidelijk zijn. Cloudoplossingen maken werken eenvoudiger, maar zonder overzicht ontstaat snel shadow IT, wat risico's vergroot zonder dat het direct zichtbaar is.

SIGNALEN DAT JE ACHTER DE FEITEN AANLOOPT

Signalen om bij stil te staan

- ☐ Weet je zeker dat back-ups getest zijn?
- ☐ Hebben ex-medewerkers nog toegang?
- ☐ Is MFA overal actief?
- ☐ Is het incident response plan ooit geoefend?
- ☐ Zijn systemen aantoonbaar up-to-date?
- ☐ Worden medewerkers getraind in phishingherkenning?

Twijfel bij één of meer vragen is een belangrijk signaal.

niceCloud

NiceCloud. Deskundig geregeld. Met plezier gedaan.

VAN INZICHT NAAR RUST EN GRIP OP JE CYBER SECURITY

De meeste organisaties die ik spreek, hadden achteraf liever eerder het gesprek gevoerd.

Niet omdat ze alles verkeerd deden, maar omdat ze signalen te laat serieus namen.

Als deze checklist vragen oproept of meerdere aandachtspunten laat zien, dan is dat geen toeval. Dat is vaak het moment waarop uitstel meer risico oplevert dan actie.

Wil je voorkomen dat keuzes pas onder druk worden gemaakt, dan is dit een logisch moment om te sparren.

Samen brengen we overzicht aan en bepalen we wat nu echt nodig is.

EVEN SPARREN?

Ron Laurens
IT-strateeg

Mobiel: +31 68 277 11 59

Kantoor: +31 88 0400 900

E-mail: r.lourens@nicecloud.nl

niceclouds

NiceCloud. Deskundig geregeld. Met plezier gedaan.

niceCloud

TROTS PARTNER VAN:

Microsoft Solutions Partner
Modern Work

Excellence Partner | kpn

NiceCloud. Deskundig geregeld. Met plezier gedaan.