Whitepaper
7 IT-fouten die het MKB duizenden euro's per jaar kosten

En hoe u ze eenvoudig voorkomt

Index

1. Inleiding

IT is voor de meeste MKB-organisaties net als elektriciteit: als het werkt, kijkt niemand ernaar om. Tot het uitvalt.
In de praktijk zien we dat veel MKB-bedrijven wel investeren in hardware, software en cloud, maar dat:

- Structuur ontbreekt
- Beveiliging versnipperd is
- Verantwoordelijkheden onduidelijk zijn
- Belangrijke processen niet zijn vastgelegd

Het resultaat: **onvoorziene kosten, uitval, beveiligingsrisico's en frustratie bij medewerkers.**

In deze whitepaper bespreken we **7 veelvoorkomende IT-fouten** in het MKB die samen jaarlijks **duizenden euro's** kunnen kosten. Voor elke fout laten we zien:

- Hoe u deze herkent
- Wat het risico en de kosten zijn
- Welke praktische stappen u vandaag al kunt zetten

Nimbus-IT ondersteunt dagelijks MKB-bedrijven bij het inrichten, beveiligen en beheren van hun IT-omgeving. De voorbeelden in deze whitepaper zijn gebaseerd op **echte situaties** die wij in de praktijk zijn tegengekomen (geanonimiseerd).

Nimbus-IT voert jaarlijks tientallen IT-scans uit bij MKB-bedrijven in Nederland. In meer dan **80%** van de gevallen vinden wij dezelfde structurele problemen. Deze whitepaper bundelt de 7 meest voorkomende fouten en biedt oplossingen die direct toepasbaar zijn, zonder grote investeringen.

2. Geen betrouwbare (en geteste!) back-up

Veel bedrijven vertrouwen blind op hun back-ups. Tot het misgaat.
Tijdens IT-scans zien wij vaak:

- Back-ups die wel draaien maar onvolledig zijn
- Restore-tests die jaren niet zijn uitgevoerd
- Back-ups opgeslagen op hetzelfde netwerk (waardoor ransomware deze verwijdert)
- NAS-systemen die niet geschikt zijn voor bedrijfscontinuïteit
- Geen versiebeheer, waardoor bestanden maar één dag of week terug kunnen

2.1 Waarom dit fout gaat

Back-ups worden vaak doorgevoerd als “inrichtingstaak”, niet als doorlopende strategie. Daardoor ontbreekt monitoring, rapportage en verificatie.

2.2 Schade bij falende back-up

- Dataverlies → productiestop
- Spoedherstel → €1.000–€10.000
- Ransomware → volledig bedrijfsstilstand
- Juridische risico’s → AVG-boetes

Een enkel incident kan **€5.000 tot €150.000** kosten.

2.3 Oplossingen

- 3-2-1-strategie: 3 kopieën, 2 verschillende media, 1 offsite
- Maandelijkse test restore
- Monitoring met automatische alerts
- Back-up-onafhankelijk van het bedrijfsnetwerk
- Heldere RPO (data) en RTO (hersteltijd)

3. Geen multi-factor authenticatie (MFA) — de grootste oorzaak van hacks

Wachtwoorden zijn de zwakste schakel in elke organisatie.
85% van alle datalekken begint met misbruik van wachtwoorden.

Zonder MFA heeft een hacker toegang tot:

- Mail
- SharePoint / OneDrive
- Teams
- Boekhoudpakketten
- CRM
- VPN
- Cloud servers
- Back-ups (!)

3.1 Hoe *snel dit misgaat*

Hacken hoeft niet technisch te zijn.
Een phishingmail is voldoende. Een wachtwoord lekt via:

- Nep-inlogpagina
- Externe website
- Ex-medewerker
- Onversleutelde wifi
- Dark web dumps
- Zodra een hacker binnen is, breidt hij in stilte zijn toegang uit.

3.2 Schade bij een hack zonder MFA

- Gestolen data
- Uitval van systemen
- Reputatieschade
- Juridische meldplicht
- Mogelijke boetes
- Kosten lopen al snel op van **€2.500 tot €50.000**.

3.3 Oplossingen

- MFA verplicht voor alle medewerkers
- Aparte admin-accounts
- Conditional Access (blokkeren onbekende landen / risicovolle devices)
- Wachtwoordrotatie + manager
- Dark web monitoring

4. Verouderde hardware en software — stille kostenpost voor MKB

Veel MKB-omgevingen draaien op:

- Servers van 5–10 jaar oud
- Windows-installaties zonder patches
- Firewalls zonder licentie
- NAS-systemen met consumenten-schijven
- Onbeheerde switches

4.1 Wat gaat hier mis?

- Hardware veroudert → hogere kans op uitval
- Software veroudert → bekende lekken worden misbruikt
- Performance daalt → medewerkers verliezen tijd
- Onderhoud is duurder → leveranciers ondersteunen het niet meer

4.2 Verborgen kosten

- Downtime: €500–€5.000 per uur
- Langzame systemen: productiviteitsverlies van 5–15%
- Spoedreparaties zijn duurder dan preventief vervangen
- Onnodige licentiekosten

4.3 Oplossingen

- Hardware vernieuwingscyclus van 3–5 jaar
- Software patchbeleid + Intune
- Monitoring op hardware status
- Migratie naar Cloud waar mogelijk
- Proactief adviesrapport per kwartaal

5. Geen centraal IT-beheer: leveranciers wijzen naar elkaar

In het MKB ontstaat vaak een versnipperde IT-situatie:

- Eén partij voor internet
- Eén partij voor telefonie
- Eén voor printers
- Eén voor Microsoft 365
- Eén voor servers
- Eén voor websites

Bij storingen ontstaat chaos. Niemand voelt zich verantwoordelijk.

5.1 Gevolg

- Trachtijden lopen op
- Problemen blijven liggen
- Kosten stijgen
- Veiligheid is moeilijk te bewaken
- Medewerkers worden gefrustreerd
- Directie heeft geen overzicht

5.2 Schade

- Inefficiënte uren
- Vertragingen in projecten
- Herstelkosten
- Geen prioriteitenplan
- Geen heldere kostenstructuur

5.3 Oplossingen

- Eén MSP (Managed Service Provider) als single point of contact
- SLA’s met responstijden
- Proactieve monitoring
- Maandelijkse rapportage
- Jaarlijkse roadmap

6. Thuiswerken zonder beveiliging — een open deur voor cybercriminelen

- Sinds hybride werken is de norm, gebruiken medewerkers vaak:
- Privé-laptops zonder beveiliging
- Onveilige thuisnetwerken
- Geen updates
- Onbeveiligde USB-opslag
- Bestanden via WhatsApp of Gmail

6.1 Risico's

- Datadiefstal
- Malware op privéapparaat
- Onbeveiligde toegang tot bedrijfsdata
- Geen zicht op wat medewerkers delen of opslaan

6.2 Kosten

- Datalekprocedures
- Meldplicht bij AP
- Juridische kosten
- Reputatieschade

6.3 Oplossingen

- Intune / MDM-beheer
- Device compliance regels
- Bedrijfsdata in beveiligde apps (geen lokale opslag)
- Encryptie verplicht
- Privé-apparaten isoleren via App Protection Policies

7. Geen goed onboarding/offboarding-proces

In veel scans zien wij:

- Actieve accounts van ex-medewerkers
- Toegang tot SharePoint van oud-medewerkers
- Doorlopende licenties (Microsoft 365, CRM, etc.)
- Enablement van extern delen zonder controle
- Toegang tot mailboxen die nooit worden gesloten

7.1 Wat is het risico?

- Data kan bewust of onbewust meegenomen worden
- Ex-medewerkers kunnen systemen blijven benaderen
- Licentiekosten stijgen onnodig

7.2 Kosten

- €300–€1.500 per medewerker per jaar aan verspilde licenties
- Schade door datalekken
- Complianceproblemen

7.3 Oplossingen

- Standaard onboarding/offboarding checklist
- Automatische provisioning via Azure AD / Intune
- Automatische deprovisioning bij offboarding
- Monthly Access Review

8. Geen monitoring, logging of inzicht — problemen worden pas ontdekt als het te laat is

Veel MKB-bedrijven draaien zonder enige vorm van monitoring. Daardoor blijft onzichtbaar:

- Back-ups die mislukken
- Inbraakpogingen
- Vollopende schijven
- Overbelasting servers
- Foutmeldingen Microsoft 365
- Misbruik accounts
- Failing hardware

8.1 Waarom dit gevaarlijk is

Problemen escaleren pas wanneer het zichtbaar wordt voor gebruikers — maar dan is het te laat.

8.2 Schade

- Spoedherstel (duur)
- Onnodige downtime
- Dataverlies risico
- Hogere beheerkosten

8.3 Oplossingen

- 24/7 monitoring & alerting
- Endpoint monitoring
- Microsoft Secure Score + Defender
- Log-analyse
- Maandelijkse IT-rapportage met advies

9. Conclusie

Deze zeven IT-fouten komen in bijna elke MKB-organisatie voor. Vaak niet door onwil, maar door tijdgebrek, versnipperde verantwoordelijkheid en beperkte inzichten. Door deze fouten te herkennen en structureel op te lossen:

- Verlaagt u risico's
- Voorkomt u datalekken
- Verhoogt u productiviteit
- Bespaart u op licentie- en hardwarekosten
- Stelt u uw bedrijf beter in voor groei

Nimbus-IT helpt bedrijven om moderne, veilige en toekomstbestendige IT-omgevingen te realiseren — zonder ingewikkelde trajecten.

Gratis IT-Omgevingsscan

Wilt u weten of deze fouten voorkomen in uw organisatie?

U ontvangt binnen 48 uur een rapport met:

- Uw grootste risico's
- Concreet verbeteradvies
- Security score
- Mogelijke kostenbeparingen

Vraag uw gratis IT-scan aan via email of bel.

10. Contact

Nimbus Cloudworks B.V.
info@nimbus-it.nl
+31 6 100 855 86
www.nimbus-it.nl