WHITEPAPER

Cybersecurity zonder gedoe

Hoe organisaties slimmer beschermen, sneller herstellen en veilig groeien

Praktische inzichten voor MKB, zorg, onderwijs en zakelijke organisaties die risicoâ€™s willen beperken zonder onnodige complexiteit.

Cybersecurity raakt meer dan IT

De tijd dat cybersecurity een puur technisch IT-vraagstuk was, ligt ver achter ons. In de huidige digitale economie is elke organisatie fundamendeel afhankelijk van data, systemen en verbonden medewerkers. Een hapering in deze keten treft direct het hart van de bedrijfsvoering.

Toch heerst er vaak onduidelijkheid. Beslissers verdwalen in technisch jargon en complexe implementatietrajecten, waardoor noodzakelijke stappen worden uitgesteld. Dit document snijdt door de ruis heen en biedt een helder, uitvoerbaar perspectief op moderne beveiliging.

De directe impact van een cyberincident:

1. Omzet

Wanneer systemen stilliggen, stopt de productie of dienstverlening. Gemiste uren vertalen zich direct in meetbaar omzetverlies.

2. Reputatie

Het uitlekken van (klant)data of het niet kunnen leveren van diensten schaadt het vertrouwen, wat jaren kost om op te bouwen.

3. Stilstand

Kritische bedrijfsprocessen vallen stil. De focus verschuift volledig van groei naar crisismanagement en schadebeperking.

4. Stress

Een incident legt enorme druk op de directie en medewerkers. De onzekerheid over herstel vreet energie en focus.

De blinde vlekken in moderne organisaties

Risico's groeien vaak onzichtbaar. Terwijl de organisatie zich richt op de dagelijkse gang van zaken, ontstaan er gaten in het digitale fundament. Het zijn zelden geavanceerde hackers die de meeste schade aanrichten; vaker is het een opeenstapeling van alledaagse kwetsbaarheden.

Phishing & Menselijke Fouten

Cybercriminelen richten zich op medewerkers via misleidende e-mails. Ã‰Ã©n onoplettende klik kan systemen compromitteren.

Zwakke Wachtwoorden & Toegang

Hergebruikte of zwakke wachtwoorden, zonder Multi-Factor Authenticatie (MFA), vormen een open voordeur voor aanvallers.

Verouderde Software

Applicaties en besturingssystemen die niet tijdig worden geÃ¼pdatet, bevatten bekende gaten die geautomatiseerd worden misbruikt.

Ontbreken van Cloud Back-ups

Vertrouwen op de cloud is goed, maar zonder externe, geÃ¯soleerde back-up ben je bij ransomware alsnog al je data kwijt.

Geen Actieve Monitoring

Zonder 24/7 monitoring hebben aanvallers vaak wekenlang onopgemerkt toegang tot het netwerk voordat ze toeslaan.

De verborgen kosten van incidenten

Wanneer organisaties de kosten van cybersecurity overwegen, vergeten ze vaak de kosten van het niet of onvoldoende beveiligen in kaart te brengen. Een incident is een kettingreactie.

1. Het Incident (bijv. Ransomware)

â†“

2. Directe Stilstand

Systemen op slot, medewerkers kunnen niet werken, communicatie valt uit.

â†“

3. Omzetverlies

Lopende orders stagneren, nieuwe aanvragen worden gemist, facturatie loopt vertraging op.

â†“

4. Reputatieschade

Klanten worden geÃ¯nformeerd over dataverlies. Vertrouwen loopt een onzichtbare deuk op.

â†“

5. Hoge Herstelkosten

Kosten voor IT-forensisch onderzoek, herstel van data, boetes (AVG) en juridische bijstand.

Een samenhangend veiligheidssysteem

Ouderwetse antivirussoftware probeert alleen te voorkomen. De moderne realiteit is dat 100% preventie onmogelijk is. Daarom hanteren we een holistische aanpak opgebouwd uit vier lagen. Pas wanneer deze lagen samenwerken, ontstaat er echte controle en rust.

1. Voorkomen (Preventie)

Het fundament: het blokkeren van bekende bedreigingen voordat ze binnenkomen. Dit omvat next-gen antivirus, firewalls, MFA, patchmanagement en medewerker-awareness. Doel is de voordeur stevig op slot te draaien.

2. Detecteren (Monitoring)

Wat als een aanvaller de voordeur passeert? Moderne Endpoint Detection & Response (EDR) systemen zoeken continu naar verdacht gedrag op werkplekken en servers, in plaats van alleen naar bekende virussen.

3. Reageren (Response)

Zodra afwijkend gedrag is gedetecteerd, moet er onmiddellijk worden gehandeld. Verdachte processen worden automatisch geÃ¯soleerd of gestopt door het Security Operations Center (SOC), voordat de schade escaleert.

4. Herstellen (ContinuÃ¯teit)

Mocht data corrupt raken of verwijderd worden (bijv. door ransomware of menselijke fouten), dan is een geÃ¯soleerde, onveranderlijke back-up cruciaal. Snelle herstelprocedures zorgen dat de bedrijfsvoering weer direct verder kan.

ZELFEVALUATIE

Waar staat jouw organisatie? (Maturity Check)

Beoordeel de huidige volwassenheid van jullie cybersecurity. Kruis aan wat reeds structureel en aantoonbaar is ingericht binnen de organisatie.

Status	Beveiligingscriterium	Toelichting
â—	**Multi-Factor Authenticatie (MFA)**	Ingeschakeld voor alle kritische systemen, cloud-omgevingen en VPN's.
â—	**Moderne Werkplekbeveiliging (EDR)**	Meer dan standaard antivirus; actieve gedragsanalyse op apparaten.
â—	**GeÃ¯soleerde Cloud Back-ups**	Microsoft 365 data (Teams, Mail, SharePoint) wordt meermaals per dag extern geback-upt.
â—	**24/7 Monitoring & Alerts**	Systemen worden continu bewaakt op verdachte inlogpogingen of data-export.
â—	**Patchmanagement**	Updates voor software en besturingssystemen worden geautomatiseerd en geforceerd uitgerold.
â—	**Security Awareness**	Medewerkers worden periodiek getraind en getest op het herkennen van phishing.
â—	**Incident Response Plan**	Het is voor iedereen duidelijk wie wat doet in de eerste minuten na een digitaal incident.

Niet alle vinkjes kunnen zetten?

Breng in kaart waar jullie exacte kwetsbaarheden zitten. Ga naar **hello.itym.nl/cybersecurity/quickscan/** of scan de QR code.

IMPLEMENTATIE

In 3 maanden naar gecontroleerde veiligheid

Het verhogen van de digitale weerbaarheid hoeft geen complex of ontwrichtend IT-project te zijn. ITYM hanteert een gefaseerde, pragmatische roadmap. Zonder ingewikkeld jargon, maar met direct resultaat en behoud van productiviteit.

Week 1: Inventarisatie & Quickscan

We starten met een heldere nulmeting. Waar staat de data? Wie heeft toegang? Wat zijn de acute risico's? Binnen een week leveren we een overzichtelijk advies zonder technische ruis.

Maand 1: De Basis op Orde

De fundering wordt gelegd. We implementeren moderne werkplekbeveiliging (EDR) op alle laptops en servers, sluiten de "voordeur" met MFA beleid en dichten bekende softwarelekken.

Maand 2: Herstel & ContinuÃ¯teit

We verzekeren de bedrijfscontinuÃ¯teit door solide, onveranderlijke back-ups in te richten voor Microsoft 365 (Teams, SharePoint, OneDrive, Mail) en bedrijfsapplicaties. Getest en veilig.

Maand 3: Actieve Monitoring & Optimalisatie

De omgeving wordt aangesloten op ons Security Operations Center (SOC). Vanaf nu wordt de infrastructuur 24/7 bewaakt op afwijkend gedrag, inclusief periodieke rapportages voor de directie.

Jouw bedrijf beschermd. Vandaag en morgen.

Van basisbeveiliging tot volledige cyberweerbaarheid â€” in heldere pakketten die passen bij jouw risicoprofiel, groeifase en behoefte aan ondersteuning.

BASIS SECURITY

Beschermd werken

Voor organisaties die een sterke, moderne basis willen zonder complexiteit.

- â€¢ Werkplekken continu bewaakt op verdachte activiteiten
- â€¢ Automatische blokkering van malware en virussen
- â€¢ Dreigingen realtime gedetecteerd
- â€¢ Geen complexe installatie â€” direct inzetbaar

Resultaat: een veilig fundament voor iedere werkplek.

ADVANCED SECURITY

Voorkomen Ã©n herstellen

Voor organisaties die niet alleen beschermd willen zijn, maar ook zeker willen herstellen.

- â€¢ Alles uit Basis Security
- â€¢ Microsoft 365 back-ups, dagelijks en herstelbaar
- â€¢ Geavanceerde dreigingsdetectie op basis van gedrag
- â€¢ Proactieve alerts en rapportages

Resultaat: minder risico op dataverlies en sneller terug in control.

COMPLETE SECURITY

Volledige ontzorging

Voor organisaties waar stilstand direct geld kost en 24/7 zicht nodig is.

- â€¢ Alles uit Advanced Security
- â€¢ 24/7 bewaking door security-specialisten
- â€¢ Aanvallen direct gestopt, niet alleen gemeld
- â€¢ Persoonlijk aanspreekpunt voor security-vragen

Resultaat: alsof je een eigen security-team hebt, zonder extra FTE.

AANVULLEND CONTINUÃ¯TEITSPAKKET

Binnen 1 uur weer online

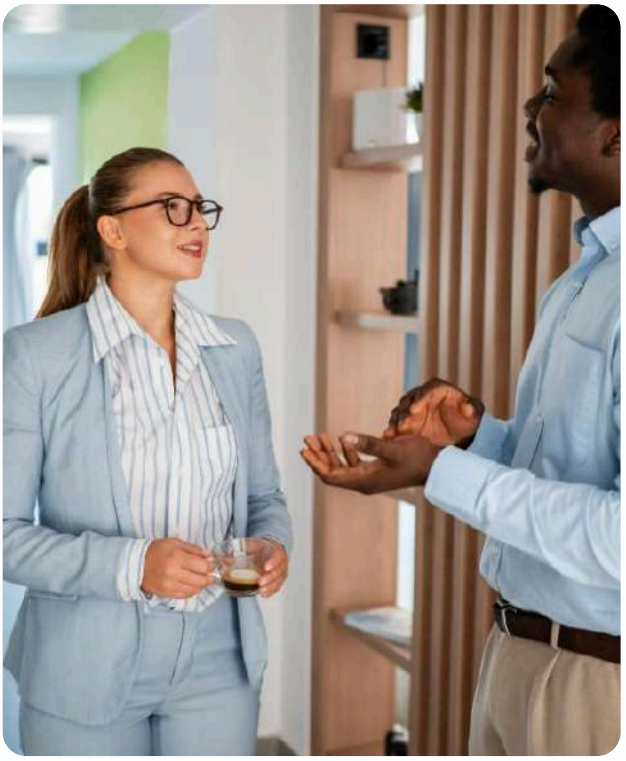
Voor als het ondanks alles toch misgaat. Combineer dit pakket met elke securitylaag voor maximale zekerheid en minimale impact op klanten, omzet en operatie.

- â€¢ Herstel van systemen binnen 60 minuten
- â€¢ Volledige back-up en disaster recovery
- â€¢ Direct actieplan bij elk type incident
- â€¢ Begeleiding bij crisis en continuÃ¯teit

Een partner die levert als het telt

Cybersecurity draait om techniek, maar valt of staat met de mensen erachter. ITYM combineert hoogwaardige technologie met een persoonlijke, no-nonsense aanpak. We kennen de dynamiek van Nederlandse zakelijke organisaties, het onderwijs en de zorg.

- **Persoonlijk contact:** Vaste specialisten die uw IT-omgeving en bedrijfsdoelen door en door kennen.
- **Voorspelbare kosten:** Een transparant, vast maandbedrag per gebruiker. Geen verborgen uurtje-factuurtje.
- **Direct inzetbaar:** Kant-en-klare oplossingen zonder slopende, langdurige IT-projecten.
- **Schaalbaar:** De beveiliging groeit moeiteloos mee met de uitbreiding van uw organisatie.



Bewezen kwaliteit en compliance

Onze processen en oplossingen voldoen aan de hoogste eisen voor informatiebeveiliging en kwaliteitsmanagement.

VOLGENDE STAP

Ontdek in 15 minuten waar je winst kunt pakken.

Klaar om jouw organisatie Ã©cht veilig te laten groeien? Plan direct het gesprek dat past bij jouw vraag â€” algemeen met Boaz of specialistisch met Fred.

Antwoord binnen 1 werkdag | **Nederlandstalig team** | **Geen salespraat**

Algemene vragen

Boaz

Voor een eerste inventarisatie, pakketvergelijkingen en praktisch advies over wat het beste past bij jouw organisatie.

Specialistische securityvragen

Fred

Voor specialistische vragen over dreigingsdetectie, SOC, incident response en continuÃ¯teit binnen jouw organisatie.

Liever dat wij contact met jou opnemen?

Meer weten? Ga naar **hello.itym.nl/contact** of scan de QR code.