JUSTDATA
Full service ict beheer

Hoe veilig is jouw IT-infrastructuur?

Cybercriminaliteit neemt snel toe en vormt voor bedrijven van elke omvang een groeiend risico. Of je nu ondernemer bent in het MKB of verantwoordelijk voor de IT-afdeling van een grotere organisatie, het bewaken van jouw IT-infrastructuur is essentieel.

Een effectieve cybersecurity-checklist helpt je om potentiële kwetsbaarheden te identificeren en deze proactief aan te pakken. In deze blog krijg je een duidelijke checklist om te beoordelen hoe veilig jouw IT-omgeving écht is.

Sterke wachtwoorden en multi-factor authenticatie (MFA)

Zwakke wachtwoorden zijn nog steeds een van de grootste kwetsbaarheden. Zorg ervoor dat jouw organisatie beleid heeft voor sterke, unieke wachtwoorden en maak gebruik van multi-factor authenticatie om de beveiliging van gebruikersaccounts aanzienlijk te versterken.

Regelmatige updates en patches

Cybercriminelen profiteren vaak van bekende kwetsbaarheden. Zorg ervoor dat alle software, besturingssystemen en applicaties regelmatig worden bijgewerkt met de nieuwste patches. Maak gebruik van automatische updates waar mogelijk.

Firewall en antivirussoftware

Een goede firewall en betrouwbare antivirussoftware vormen de basis van elke cybersecurity-strategie. Controleer regelmatig of deze beveiligingslagen actief zijn en goed functioneren, en pas indien nodig configuraties aan op veranderende dreigingen.

Data-backups

Het regelmatig maken van back-ups is cruciaal om gegevensverlies bij ransomware of andere cyberincidenten te voorkomen. Zorg ervoor dat back-ups regelmatig worden getest en bewaard op veilige, externe locaties.

Toegangscontrole en rechtenbeheer

Niet iedere medewerker hoeft toegang te hebben tot gevoelige bedrijfsgegevens. Implementeer strikte toegangscontrole en beperk rechten volgens het principe van 'least privilege'. Herzie rechten en toegang regelmatig om misbruik en risico's te beperken.

Beveiligde netwerkverbindingen (VPN)

Met de toename van thuiswerken zijn VPN's essentieel geworden. Zorg ervoor dat medewerkers uitsluitend via beveiligde verbindingen toegang krijgen tot het bedrijfsnetwerk en stel duidelijk beleid op voor het gebruik van openbare wifi-netwerken.

Awareness-trainingen voor medewerkers

Medewerkers zijn vaak de zwakste schakel in cybersecurity. Regelmatige training en bewustwording rondom phishing, social engineering en andere cyberdreigingen zorgen ervoor dat je team deze bedreigingen vroegtijdig herkent en voorkomt.

Incidentresponsplan

Een effectief incidentresponsplan is essentieel om snel en effectief te reageren bij cyberincidenten. Zorg dat dit plan duidelijk is en dat alle relevante partijen precies weten welke acties zij moeten ondernemen in geval van een incident.

Periodieke security audits

Een onafhankelijke security audit helpt bij het ontdekken van blinde vlekken in je IT-beveiliging. Overweeg jaarlijks of halfjaarlijks een audit uit te voeren om je beveiligingsmaatregelen te toetsen en te versterken.

Monitoring en detectie

Maak gebruik van geavanceerde monitoringtools om verdachte activiteiten in je IT-infrastructuur tijdig op te sporen. Snelle detectie van dreigingen verkleint de kans op ernstige schade aanzienlijk.

Conclusie

Het regelmatig controleren van deze cybersecurity-checklist helpt jouw organisatie om adequaat beschermd te blijven tegen cyberaanvallen. Neem cybersecurity serieus en voorkom financiële schade, reputatieverlies en downtime door cyberincidenten. Zorg ervoor dat jouw bedrijf proactief handelt en altijd klaar staat om te reageren op de continu veranderende dreigingen.

Meer weten?

Justcloud365 wordt continu doorontwikkeld om aan de wensen, vragen, behoeften en uitdagingen van onze klanten tegemoet te komen. Meer weten over Justcloud365? Of benieuwd naar welke (andere) oplossing geschikt is om jouw organisatie te laten groeien? Neem gerust contact met ons op!

Paul Kremer

E-mail : paul@justdata.nl

Telefoon: 0320 – 76 76 76