

Het cyberrisico beheersbaar maken - een stappenplan

De hoge kans op cyberaanvallen wordt gezien als een van de grootste bedreigingen voor bedrijven. Om deze kans zo klein mogelijk te maken, is het belangrijk om je bedrijf weerbaarder te maken met onderstaande tips.

- **Multi-Factor Authentication (MFA)**
Door multi-factor authenticatie af te dwingen op elk apparaat in je netwerk voorkom je toegang van kwaadwillenden.
- **Managed Detection and Response (MDR)**
MDR is een service die je infrastructuur dag en nacht beschermt. Eye Security levert MDR-service om aanvallen te detecteren en snel te reageren.
- **Regelmatige updates en patches**
Door software regelmatig bij te werken, verhelp je bekende kwetsbaarheden en sluit je toegangspoorten voor aanvallers.
- **Beveiligde back-ups**
Back-ups kunnen van cruciaal belang zijn voor je bedrijf. Bij een aanval kan namelijk teruggelopen worden op de back-ups mochten deze nog beschikbaar zijn.
- **Incident Response Plan**
Hoewel het doel is om nooit slachtoffer te worden van een cyberaanval, is het belangrijk om je voor te bereiden op een incident om de impact te beperken.
- **Medewerkers Awareness Training**
Regelmatige awareness trainingen helpen medewerkers phishing e-mails te herkennen. Deze trainingen maken deel uit van het aanbod van Eye Security.
- **System & Cloud Security Configuratie**
Je werkstations, servers en cloud moeten volgens de security standaarden zijn beveiligd en geconfigureerd.

Meer informatie?

Eye Security biedt een betaalbaar totaalpakket om je cyberrisico beheersbaar te maken. Maak je je zorgen over je cyberweerbaarheid? Neem contact op met Eye Security via [onze website](#).

