Checklist Cyberweerbaarheid

PRIVACY OP SCHOOL

Voorkom dat je school wordt gehackt!

Steeds vaker hoor je in het nieuws dat organisaties gehackt worden en geen toegang meer hebben tot hun eigen data. Het gevolg is dat er een groot geldbedrag wordt geëist om weer toegang te krijgen tot de digitale schoolomgeving. Hackers zetten organisaties vaak onder druk door te dreigen persoonsgegevens openbaar te maken, waardoor vervolgens zomaar honderden persoonsgegevens van medewerkers en leerlingen op straat liggen.

Hoe blijf je ransomware aanvallen de baas en blijf je in controle over je data? De volgende checklist helpt je hierbij.
Kan je overal een vink zetten? Dan ben je goed op weg!

- [ ] Zet 2-factor authenticatie aan voor gebruikers van applicaties met bijzondere persoonsgegevens.
- [ ] Zet encryptie (versleuteling) aan voor applicaties met bijzondere persoonsgegevens.
- [ ] Pas segmentatie (technische scheiding) van netwerken en applicaties toe (doe dit proactief).
- [ ] Wijzig standaard wachtwoorden, maak wachtwoordzinnen, gebruik een wachtwoordmanager.
- [ ] Stel toegangsrechten in voor applicaties (niet iedereen hoeft overal bij te kunnen).
- [ ] Maak back-ups (en sla deze apart van je schoolomgeving op).
- [ ] Gebruik uitsluitend software van erkende leveranciers.
- [ ] Zorg dat incidentmanagement op orde is en er een noodplan klaar ligt.
- [ ] Vernietig persoonsgegevens conform de bewaartermijnen (denk ook aan de mailbox).
- [ ] Wijs medewerkers op de gevaren. Zorg dat ze weten wat ze moeten doen bij een aanval.
- [ ] Inventariseer kwetsbaarheden en test of de maatregelen afdoende zijn.
- [ ] Stel een security officer aan.
- [ ] Voer regie op datakoppelingen en zorg dat de juiste IBP-richtlijnen* worden toegepast.
- [ ] Zorg dat incidentmanagement op orde is en er een noodplan klaar ligt.

*Informatiebeveiliging en privacy