Cybersecurity

Cybercriminaliteit vormt een steeds grotere bedreiging voor de continuïteit van een bedrijf, kliniek of instelling. Door het stelen van gegevens (data theft), door het versleutelen van bestanden (ransomware) of door het platleggen van de website (DDos) kunnen criminelen ernstige schade toebrengen.

Preventieve beveiligingsmaatregelen

- Inventariseer welke gegevens in de administratie als persoonsgegeven aangemerkt moeten worden.
- Stel regels op waaraan iedereen zich moet houden als ze omgaan met die gegevens.
- Denk bij uitwisseling van gegevens goed na of de persoonsgegevens wel nodig zijn. Anonimiseer gegevens indien mogelijk.
- Zorg dat het bovenstaande bij iedereen bekend is.
- Zorg dat alleen mensen die de persoonsgegevens moeten gebruiken bij die gegevens kunnen en alle anderen dus niet.
- Stel goede sterke wachtwoorden in en vervang die van tijd tot tijd.
- Deel wachtwoorden met niemand, ook niet intern.

Zorg voor de volgende technische maatregelen:

- Maak regelmatig backups van de belangrijke gegevens, waaronder de persoonsgegevens.
- Bewaar die backups apart, dus niet op het netwerk of de PC zelf.
- Zorg dat alle apparatuur up-to-date is met alle security-patches.
- Zorg dat alle software up-to-date is met security-patches;
- Installeer goede anti-malwaresoftware en zorg dat die up-to-date blijft.
- Zorg voor beveiliging van de internetaansluiting. Dat kan door firewall-software te installeren op de PC. Maar u kunt ook de router van uw provider door een specialist laten configureren. Of, zeker bij grotere netwerken, installeer een aparte firewall.
- Zorg dat er geen 'default'-wachtwoorden op uw apparatuur voorkomen.
- Zorg dat uw website goed beveiligd is, zeker als mensen er gegevens kunnen bekijken, invoeren en bewerken.
- Maak bij losse gegevensdragers (USB-sticks, externe harddisks, CD's en DVD's) gebruik van encryptie (versleuteling), zeker als u die gegevensdragers meeneemt of opstuurt.
- Zorg dat persoonsgegevens niet (automatisch) worden gesynchroniseerd naar cloud-opslag (OneDrive en iCloud).
- Maak bij elektronische uitwisseling (Email, WeTransfer, Dropbox) van persoonsgegevens gebruik van encryptie.

Een goed pakket aan maatregelen

1. Preventiemaatregelen treffen
2. Detectie, opsporing
3. Herstel van data en gegevens

Tips

√ Laat u adviseren door een specialist.

√ Bekijk de mogelijkheden van de Cyber en Data Risks verzekering. Met name als het gaat om detectie en herstel zal niet elke instelling, kliniek of praktijk hier zelf toe in staat zijn.

"Meldplicht datalekken" vanaf 1 januari 2016

Sinds 1 januari 2016 geldt de meldplicht datalekken, als onderdeel van de Wet bescherming persoonsgegevens. De Autoriteit Persoongegevens ziet erop toe of organisaties zich houden aan de wet- en regelgeving voor het gebruik van persoonsgegevens.

De Autoriteit Persoonsgegevens heeft vergaande mogelijkheden om boetes op te leggen, die kunnen oplopen tot 820.000 euro. En dat houdt de gemoederen flink bezig.

Een boete zal alleen worden opgelegd als u verwijtbaar tekort schiet bij de omgang met en de beveiliging van persoonsgegevens. **Onzorgvuldig gedrag** is een aandachtspunt en de **beveiliging van gegevens** een tweede aandachtspunt.

Jan de Jager (riskmanager VvAA) en
Paul van de Berg (security officer VvAA)