**Beveiliging & Wetgeving – Documentatie voor IT-omgevingen**

**1. 🔐 Wat is IT-beveiliging?**

**IT-beveiliging**, ook wel **cybersecurity**, is het geheel van maatregelen en technologieën die ervoor zorgen dat digitale systemen, netwerken en gegevens beschermd zijn tegen ongewenste toegang, misbruik, verlies of vernietiging. Beveiliging bestaat uit verschillende domeinen:

**Belangrijkste beveiligingsdomeinen:**

* **Fysieke beveiliging**: bescherming van hardware, servers en netwerkinfrastructuur (bv. sloten, camerabewaking).
* **Netwerkbeveiliging**: bescherming tegen indringers, virussen en datalekken (bv. firewalls, VPN).
* **Toegangsbeheer**: zorgen dat enkel bevoegde personen toegang krijgen tot data of systemen (bv. wachtwoorden, 2FA, RBAC).
* **Gegevensbescherming**: encryptie, back-ups en gegevensherstel.
* **Continuïteitsbeheer**: planning voor noodsituaties (disaster recovery).
* **Beveiligingsbeleid**: afspraken en procedures binnen een organisatie (bv. software-installatiebeleid).

**2. ⚖️ Relevante wetgeving in België & Europa**

Beveiliging is niet enkel technisch: ook de **wetgeving** speelt een belangrijke rol. Elke IT-professional moet op de hoogte zijn van deze basiswetten:

**📘 2.1 Algemene Verordening Gegevensbescherming (AVG / GDPR)**

* **Doel**: Bescherming van persoonsgegevens van Europese burgers.
* **Belangrijk artikel**: Artikel 32 – Organisaties moeten passende technische en organisatorische maatregelen nemen om persoonsgegevens te beveiligen.
* **Voorbeeld**: Als je een website maakt die klantgegevens opslaat, moet je zorgen voor versleuteling en veilige opslag.

**📘 2.2 Strafwetboek – Artikels 550bis en 550ter**

* **Artikel 550bis**: Verbiedt het opzettelijk en zonder rechtstoegang binnendringen in informaticasystemen.
* **Artikel 550ter**: Verbiedt het saboteren van systemen, zoals met DDoS-aanvallen.
* **Voorbeeld**: Een hacker die een server aanvalt zonder toestemming, is strafbaar onder deze artikelen.

**📘 2.3 NIS-wet (Netwerk- en Informatiebeveiliging) – België**

* **Van kracht sinds**: 1 juli 2022
* **Doel**: Verplicht kritieke sectoren (zoals overheden, energie, zorg) om hun IT-systemen te beveiligen en incidenten te melden.
* **Voorbeeld**: Een overheidsinstantie moet een cyberaanval melden aan het CSIRT (Computer Security Incident Response Team).

**📘 2.4 EU Cybercrime Convention (Budapest Conventie)**

* **Internationale wet** tegen cybercriminaliteit.
* Maakt het mogelijk dat Belgische rechtbanken ook buitenlandse cybercriminelen kunnen vervolgen.
* Voorbeeld: Een buitenlandse DDoS-aanval op een Belgische server valt onder deze conventie.

**3. 📄 Praktijk: Hoe pas je dit toe als IT’er?**

| **Situatie** | **Beveiligingsmaatregel** | **Wettelijk aspect** |
| --- | --- | --- |
| Werknemer verliest laptop met klantengegevens | Full-disk encryptie zoals BitLocker | Artikel 32 GDPR |
| Ex-medewerker heeft nog toegang tot bedrijfsdata | Tijdige deactivatie via Active Directory | Beveiligingsbeleid + GDPR |
| Hacker voert DDoS-aanval uit op overheidswebsite | WAF + DDOS-mitigatie | Artikel 550ter + NIS-wet |
| Je maakt een website met een contactformulier | SSL + versleutelde database | GDPR + deontologie |

**4. 📌 Conclusie**

Als IT’er is het essentieel om niet alleen technische kennis te hebben, maar ook het **juridisch kader** waarin je werkt te begrijpen. Elke handeling (zoals toegang geven, systemen onderhouden, data verwerken) moet zowel technisch correct als wettelijk verantwoord zijn.

**Belangrijke vuistregels:**

* **Toegang enkel met toestemming**.
* **Gegevens beveiligen** alsof ze van jou zijn.
* **Bij twijfel: vraag formele toestemming of documenteer je handelingen.**
* **Respecteer de privacy** van collega’s en klanten.