10 punten voor veilig servers/services beheren voor systeembeheerders

1. **Hardware en besturingssysteem** van elke server moet **doeltreffend beveiligd** zijn:

   - Het toestel staat op een **veilige locatie**:
     - beschermd tegen onrechtmatige fysieke toegang
     - beschermd tegen fysische schade als gevolg van hitte, brand, water, stof,…

   Het toestel wordt daarom in principe ondergebracht of opgezet in een centraal datacenter van de UGent.

   - Het besturingssysteem beschikt steeds over de meest recente updates.

   - Features van het besturingssysteem die nooit gebruikt worden, zijn verwijderd.

   - Onnodige services zijn uitgeschakeld.

   - Legacy besturingssystemen die niet meer ondersteund worden, mogen niet langer gebruikt worden. Daarvoor moet een migratie voorzien worden naar een systeem dat duurzame veiligheidsgaranties biedt. Maak eventueel een afspraak met de specialisten van DICT voor advies.

2. **Toepassingen** op elke server moeten **doeltreffend beveiligd** zijn:

   - Alle geïnstalleerde toepassingen beschikken over de meest recent beschikbare updates.

   - voor off-the-shelf toepassingen en componenten (add-ons) moet regelmatig (of automatisch) nagekeken of er kwetsbaarheden bekend en beschreven zijn (bv. via Common Vulnerabilities and Exposures (CVE)). Beschikbare updates en patches moeten zo snel mogelijk toegepast worden.

   - voor custom ontwikkelingen (in eigen beheer of outsourced) wordt minstens nagekeken of voldoende beveiligd is tegen de kwetsbaarheden van de Open Web Application Security Project (OWASP) Top 10, bijvoorbeeld SQL-Injection en Cross-Site Scripting.

   - Custom systemen met persoonsgegevens en vertrouwelijke informatie worden onderworpen aan een bijkomende veiligheidscontrole vooraleer in productie te gaan (in samenspraak met de informatieveiligheidsconsulent).

3. **Netwerktoegang** tot servers moet **doeltreffend beveiligd** zijn:

   - Het systeem wordt verbonden met UGentNet via een vaste (bekabelde) netwerkverbinding (LAN).

   - Beperk de toegang tot het toestel op netwerkniveau:
     - Maak bij het registreren van het toestel de juiste keuze: intranet (server UGent) of internet (server Internet). Kies enkel voor server Internet als dat voor de geplande services noodzakelijk is.
     - Laat enkel die netwerkpoorten open die nodig zijn voor de bedoelde services
     - Vermijd het internet-breed openstellen van netwerkprotocols en netwerktoepassingen die het beheer van je systeem vanop afstand mogelijk maken zoals SSH, RDP of webgebaseerde beheerstools. Open ze enkel voor specifieke subnets binnen UGentNet en voor toegang via VPN.

   - Voorzie in een voldoende niveau van intrusion detection en volg de resultaten daarvan op.

4. **Bescherm de accounts** en de daaraan gekoppelde aanmeldingsgegevens (gebruikersnaam en wachtwoord) op alle systemen

   - bescherm in het bijzonder system administrator- en root-accounts. Gebruik steeds lange, sterke wachtwoorden. Kies regelmatig een nieuw wachtwoord.

   - werk voor UGent gebruikersaccounts uitsluitend met de authenticatiemechanismen centraal aangeboden door DICT: Centrale Authenticatie Service (CAS) of Active Directory authenticatie en OAuth voor mobiele toepassingen.

   - het is verboden om zelf login-forms op te zetten waarmee UGent accountgegevens opgevraagd worden.

   - indien toch in een Web-systeem voor zelf-registratie wordt voorzien (onafhankelijk van CAS en AD), maak er de gebruikers dan op attent dat het verboden is dezelfde credentials (gebruikersnaam / emailadres en wachtwoord) te gebruiken als van het UGent account. Laat geen anonieme zelf-registratie toe.

   - Neem de nodige voorzorgen voor de beveiliging van inloggegevens. Inloggegevens moeten altijd versleuteld worden. Webauthenticatie moet dus altijd via https (en met een correct server-certificaat).

5. Wees je als systeembeheerder voldoende **bewust van courante risico's en gevaren**:

   - Servers zijn prime targets van hackers. Configureer daarom voldoende logging en monitoring en bekijk de logs en resultaten van monitoring regelmatig. Implementeer beschikbare security updates zo snel mogelijk. Blijf op de hoogte van Common Vulnerabilities and Exposures voor je systemen.

   - Wanneer vastgesteld wordt dat een server gehackt is, is het vaak zeer moeilijk om te weten te komen hoe diep het systeem gecompromitteerd werd en of er secundaire malware is opgezet (bv. remote command en control software). Daarom is het aangewezen om na een incident een clean install te doen. Hou daar al op voorhand rekening mee.

6. **Gebruik de centrale infrastructuur, platformen en toepassingen aangeboden door DICT**

   - De basisbeveiliging van de centrale infrastructuur, platformen en toepassingen aangeboden door DICT wordt gegarandeerd door de specialisten van DICT.

   - Maak voor bestaande en/of legacy systemen die nog niet centraal zijn opgesteld een afspraak met de specialisten van DICT om ze naar de centrale infrastructuur te migreren.

7. **Volg erkende best-practices voor de beveiliging van servers en services.**

   - Zoek de juiste balans tussen system hardening (tegen gekende en ongekende bedreigingen) met verschillende lagen van bescherming ("defense in depth") en een goede onderhoudbaarheid.

   - Raadpleeg security benchmarks en standaard security configuraties specifiek voor elk besturingssysteem.

8. **Lokale systeembeheerders (binnen een vakgroep, facultair of binnen centrale administratie) dragen een belangrijk stuk van de verantwoordelijkheid** voor de veiligheid van de systemen onder hun beheer, inclusief voor de veiligheid van de data die erop verwerkt wordt.

   Lokale systeembeheerders moeten daarom zelf nadenken over en verantwoordelijk omgaan met de informatieveiligheidsrisico's verbonden aan de systemen die ze beheren, in het bijzonder als die persoonsgegevens of vertrouwelijke informatie bevatten.

9. **Samen sterk**:

   - Neem het initiatief bij het begin van elk IT-project om af te stemmen met relevante stakeholders en in het bijzonder met DICT.

   - Houd contact, communiceer en overleg wanneer nodig met collega's systeembeheerders aan de UGent, de specialisten van DICT en de informatieveiligheidsconsulent.

10. **Breng de Helpdesk van DICT zo snel mogelijk op de hoogte** als je vermoedt dat een server gehackt is, of ook als je een ander **informatieveiligheidsincident** vaststelt.

    Dit is bijzonder belangrijk voor kritische systemen of systemen waarbij persoonsgegevens of vertrouwelijke informatie in de verkeerde handen terecht zouden kunnen komen.