2.9 Informatiebeveiliging

Visie op digitalisering en informatiebeveiliging

Dreigingen zijn reëel en de afhankelijkheid van ICT is groot. Wereldwijd is er sprake van een groeiende cyberdreiging, ook voor universiteiten die intensief onderzoek uitvoeren, zo blijkt uit het SURF Cyberdreigingsbeeld 2020/2021. Hoewel dit beeld niet nieuw is, wordt de impact van security-incidenten alleen maar groter. De afhankelijkheid van ICT is immers zeer groot, analoge middelen zijn bijna volledig verdwenen en er zijn maar weinig alternatieven voorhanden.

Impact van verstoringen of manipulatie van IT-systemen is groot. Uitval, verstoring of manipulatie van IT-systemen brengt voor iedere organisatie schade met zich mee. Deze schade is zowel economisch van aard bij verlies van middelen, als ook persoonlijk bij verlies van (persoons)-gegevens. Het raakt ook de reputatie van de organisatie. De UvA heeft de afgelopen jaren meerdere incidenten gekend, zoals phishing-aanvallen, oplichting van medewerkers via SMS, gestolen laptops met vertrouwelijk informatie, en de cyberaanval in februari 2021. Informatiebeveiliging is een randvoorwaarde voor de continuïteit van onderwijs en onderzoek.

Risicobewust handelen bevordert de bescherming van kernwaarden en het open karakter van de instelling. Informatiebeveiliging vormt een belangrijke pijler voor het waarborgen van de kernwaarden van de instelling. De UvA maakt zich daarom sterk voor de bescherming van haar gegevens. Om het open karakter van de instelling te kunnen blijven handhaven, is van cruciaal belang dat de informatiebeveiligingsrisico's inzichtelijk zijn en dat er bewust naar gehandeld wordt. Gebrek aan inzicht en handelingsperspectief in de organisatie, leidt tot onvoorziene risico's.

Wat we belangrijk vinden

- Dat er in de organisatie (ICTS, diensten en faculteiten) permanent aandacht is voor – en gewerkt wordt aan – het verbeteren van het niveau van informatiebeveiliging;
- Het verhogen van de digitale, operationele weerbaarheid staat voorop;
- Het verhogen van de informatiebeveiliging van zowel de door ICTS beheerde IT-systemen als van de systemen die bij faculteiten in beheer zijn;
- Goed zicht houden op de voortgang door te blijven monitoren, onder andere door elk jaar een externe audit uit te voeren.

Doelen van de digitale agenda informatiebeveiliging

- Risicobewust handelen: het tijdig inzien, voorkomen en oplossen van risico's die de kernwaarden en het open karakter van de instelling bedreigen, met de focus op de beveiliging van (persoons)gegevens;
- Verhogen van de digitale, operationele weerbaarheid: het toepassen van proportionele beveiligingsmaatregelen op mensen, processen en techniek, om risico's te minimaliseren met een integrale benadering voor faculteiten en diensten;
- Respons op incidenten: Tijdig detecteren van een doorbraak in de beveiliging en daar snel en kundig op reageren om de impact ervan te minimaliseren;
- Borging in de organisatie: het beleggen van de verantwoordelijkheid voor informatiebeveiliging in de organisatie, het bewerkstelligen van samenwerkingsverbanden binnen de organisatie, en het controleren van de naleving van het beleid. De volwassenheid van informatiebeveiliging wordt in beeld gebracht met het SURFaudit-model. De UvA streeft, met de gehele sector, naar een volwassenheidsniveau van 3 op een schaal van 1 tot 5.

Overzicht digitale agenda, focusgebied informatiebeveiliging

Wat willen we bereiken?	*Wat moeten we daarvoor doen?*	*Waar moeten we rekening mee houden?*
Risicobewust handelen		
Het tijdig inzien, voorkomen en oplossen van risico's die de kernwaarden en het open karakter van de instelling bedreigen, met de focus op de beveiliging van (persoons)gegevens.	Opzetten van IB-risicomanagement op strategisch, tactisch en operationeel niveau, en integreren met Enterprise Risk Management. Alle systemen en dataverwerkingen onderwerpen aan een risicoanalyse en vervolgende maatregelen implementeren.	Aansluiten bij risicomanagement van andere domeinen.
Verhogen van de digitale, operationele weerbaarheid		
Het toepassen van proportionele beveiligingsmaatregelen op mensen, processen en techniek, om risico's te minimaliseren met een integrale benadering voor faculteiten en diensten.	Basisset operationele maatregelen definiëren, uitbreiden en inzetten. Awareness bij medewerkers en studenten. Een veilige infrastructuur creëren met basismaatregelen. Het registreren van maatregelen bij bedrijfsmiddelen en eigenaar. Cyberweerbaarheid meetbaar maken.	Een integrale aanpak over alle faculteiten en diensten heen. Een open instelling is een aandachtspunt bij het realiseren van operationele weerbaarheid. We hebben aandacht voor het dilemma dat informatiebeveiliging ten koste kan gaan van b.v. gebruiksgemak.
Respons op incidenten		
Tijdig detecteren van een doorbraak in de beveiliging, en daar snel en kundig op reageren om de impact ervan te minimaliseren.	Versterken en professionaliseren CERT. Uitbreiden SOC-functionaliteit (Security Operation Centre). Geautomatiseerd reageren op incidenten om zo de tijdsduur te verkorten tussen aanval, detectie en oplossen.	Aanvallers werken ook buiten kantooruren.
Borging in de organisatie		
Het beleggen van de verantwoordelijkheid voor informatiebeveiliging in de organisatie, het bewerkstelligen van samenwerkingsverbanden binnen de organisatie, en het controleren van de naleving van het beleid. De UvA streeft, met de gehele sector, naar een volwassenheidsniveau van 3 op een schaal van 1 tot 5.	Inrichten adequate IB-organisatie, duidelijke governance en TVB IB-functionarissen in de afdelingen (diensten staf en faculteiten). Opleiden en coachen van IB-medewerkers en ICT-medewerkers. Herzien en uitbreiden van informatie-beveiligingsbeleid en -richtlijnen. Periodieke toetsing: externe audits, interne controles (bijvoorbeeld pentesten). Rapportage aan (senior)management op de voortgang van verbeterprogramma's, de huidige risico's en de status van de cyberweerbaarheid.	De volwassenheid van informatiebeveiliging wordt in beeld gebracht met het SURFaudit-model. Rekening houden met decentrale bevoegdheden. Standaard-werkprocessen worden op een te laag niveau uitgevoerd om de risico's in het IB-domein voldoende te kunnen mitigeren. Richtlijnen hebben betrekking op beheer van bedrijfscontinuïteit, zoals b.v. back-up-beleid en disaster recovery. Rapportages betreffen zowel diensten als faculteiten.