

DREIGINGEN HO OP HET GEBIED VAN CYBERSECURITY

Uit het cyberdreigingsbeeld voor het hoger onderwijs van 2016 blijken de topdreigingen voor het onderwijsproces 'Manipulatie van digitaal opgeslagen data' en 'Identiteitsfraude' te zijn.

Voor het onderzoeksproces zijn de topdreigingen 'Verkrijging en openbaarmaking van data' en 'Spionage'.

En voor de bedrijfsvoering wordt 'Verkrijging en openbaarmaking van data' als meest bedreigend gezien.

Spanningsveld tussen openheid en veiligheid

Het hoger onderwijs kan en wil als sector niet de poorten dichtgooien. Om goed onderzoek en onderwijs te laten gedijen is het van groot belang dat er een cultuur van openheid blijft bestaan en dat kennisuitwisseling wordt bevorderd. Aan de andere kant werken universiteiten en hogescholen hard aan het verzekeren van een zo veilig mogelijke leer- en werkomgeving.

Wat doet de HO sector eraan om zich te weren tegen cyberdreigingen?

Het hoger onderwijs zet zich in om deze dreigingen het hoofd te bieden als sector. Dit doen hogescholen en universiteiten verenigd binnen SURF onder andere op de volgende manieren:

- de professionals op het gebied van cybersecurity en privacy hebben constant contact met elkaar binnen twee actieve communities en het programma Integraal Veilig Hoger Onderwijs. Zo hoeft een instelling niet steeds het wiel opnieuw uit te vinden en kan expertise op specialistische onderwerpen het best worden benut en gedeeld;
- SURF ontwikkelt voor onderwijs- en onderzoeksinstituten campagnemateriaal dat de instellingen kunnen inzetten om de awareness van security en privacy risico's te verhogen;
- om hun weerbaarheid in het geval van een crisis te vergroten hebben in 2016 bijna dertig hogescholen en universiteiten mee gedaan aan de landelijke cyber-crisis oefening OZON;
- in de tweejaarlijkse benchmarkingronde meet de hoger onderwijssector welk volwassenheidsniveau zij heeft op het gebied van cybersecurity. De nieuwste benchmarkronde zal in 2017 plaatsvinden. Daarnaast kunnen hogescholen en universiteiten op elk gewenst een self-assessment uitvoeren en een peer review aanvragen met behulp van SURFaudit.
- opstellen van een jaarlijks cyberdreigingsbeeld dat op strategisch niveau de belangrijkste ontwikkelingen aangeeft.