CYBERSECURITY VERDIENT UW AANDACHT

SAMENWERKEN VOOR VEILIG ONDERWIJS EN ONDERZOEK

ICT-voorzieningen zijn een essentiële voorwaarde geworden voor onderwijs en onderzoek. Iedere verstoring in beschikbaarheid of betrouwbaarheid heeft een directe impact op het werk of de studie. Er moet vertrouwd kunnen worden op de opgeslagen data, zoals onderzoeksgegevens en studentcijfers, en op de beschikbaarheid van onderzoeksinstrumenten en digitale leermiddelen. Samenwerken aan cybersecurity en de weerbaarheid van de hele sector is daarom noodzakelijk voor het soepel en betrouwbaar functioneren van het onderwijs en onderzoek in Nederland en wereldwijd.

Met de toenemende afhankelijkheid van ICT in onderwijs en onderzoek wordt goed beveiligen steeds belangijker. Dat is niet slechts een technische aangelegenheid. Het is ook niet alleen een verantwoordelijkheid van de ICT-beheerders, maar van de hele organisatie. Om veilig te kunnen blijven werken, onderzoeken en leren moet iedereen zich bewust zijn van de risico's en wat je rol is om je daartegen te wapenen, van bestuurder tot eindgebruiker.

BEVEILIGING IS MEER DAN TECHNIEK

Om beveiliging goed op orde te krijgen is er aandacht nodig voor de TAO van cybersecurity: techniek, awareness en organisatie. Binnen onderwijs en onderzoek doen we dit in samenwerking omdat de uitdagingen voor bijna alle instellingen dezelfde zijn. Door samen te werken kunnen we krachten bundelen en ervaringen delen.

TECHNIEK

Technie k is als een slot op de voor- en achterdeur: zo goed mogelijk bestand tegen inbraakpogingen, maar nutteloos als het niet wordt gebruikt dus zeker niet voldo nd . Goede mailfiltering tegen spam, phishing en virussen, goed opgezette rechten en beveiliging van interne systemen is ook noodzakelijk.

AWARENESS *(bewustwording)*

Gebruikers moeten zich ervan bewust zijn dat ze een interessant doelwit zijn voor cybercriminelen en hebben ook een eigen verantwoordelijkheid in het veilig gebruik van middelen en diensten. Bewustwordingsprogramma's kunnen gebruikers helpen de gevaren te onderkennen.

ORGANISATIE

Iedereen van onder tot boven in de organisatie dient het belang van (cyber)security te erkennen. Integrale veiligheid en risicomanagement, inclusief cybersecurity, moeten regulier op de bestuurlijke agenda staan om risico's en kansen af te wegen, lering te trekken uit het verleden en investeringen te doen in de toekomst. Beheerders moeten de tijd, middelen en opleidingen krijgen om hun systemen veilig in te regelen. Bewustwordingsprogramma's moeten in samenwerking met communicatiemedewerkers worden uitgevoerd en regelmatig oefenen moet de standaard worden, vergelijkbaar met ontruimingsoefeningen en BHV.

CONTINUE AANDACHT

Continue inzet op bewustwording, organisatie en techniek is nodig om veilig te kunnen blijven werken. Van beheerder tot bestuurder en van onderzoeker tot student: iedereen speelt een rol in het veilig kunnen blijven studeren, werken en onderzoeken. Door samen te werken zijn bedreigingen beter het hoofd te bieden en blijft de impact – mocht het toch een keer misgaan – zo beperkt mogelijk

WE WERKEN AL VEEL SAMEN...

Omdat veel security-uitdagingen voor onze hele sector gelden, werken we op alle niveaus samen met de instellingen. Binnen de SCIRT-en SCIPR community's werken we samen aan operationele en technische security en aan (organisatorische) informatiebeveiliging en privacy. Op bestuurlijk niveau werken we samen binnen het Platform Integrale Veiligheid Hoger Onderwijs. We ondersteunen de instellingen ook op het gebied van digitale veiligheid door innovatieactiviteiten en diensten.

Iedere twee jaar organiseren we samen met de instellingen een grote cybercrisisoefening OZON en voor de tussenliggende jaren is een kleinschalige oefening beschikbaar. Op bestuurlijk niveau zijn er werkconferenties security & privacy opgestart. De bewustwordingscampagne ***Cybersave Yourself*** biedt instellingen een praktische toolkit voor het opzetten van een bewustwordingsprogramma voor alle eindgebruikers. Met de tweejaarlijkse benchmark informatiebeveiliging kunnen we als sector zien hoe we ervoor staan en werken aan een volwassen informatiebeveiligingbeleid.

...MAAR HET KAN NOG BETER!

- Maak integrale veiligheid, inclusief cybersecurity, en risicomanagement een vast onderwerp op de bestuursagenda.
- Zorg voor continue aandacht voor de drie pijlers (TAO) binnen alle lagen van de organisatie: benut alle technische mogelijkheden, zorg voor bewustzijn bij alle gebruikers en coördineer cybersecurity goed binnen de organisatie.
- Doe mee aan de tweejaarlijkse benchmark informatiebeveiliging om gezamenlijke uitdagingen inzichtelijk te maken.
- Werk samen en blijf oefenen.

Verder lezen:

www.surf.nl/veiligheid-op-de-bestuurstafel
www.surf.nl/cyberdreigingsbeeld-2018
www.surf.nl/whitepaper-cybercrisisoefening
www.surf.nl/surfaudit-benchmark
www.surf.nl/beveiligingscommunitys
Cybersecurityraad – Handreiking bestuurders:
https://edu.nl/436ry