Vergroot de cyberweerbaarheid van het onderwijs door beter te reageren op incidenten

In de strijd tegen cybercrime kunnen scholen tegenwoordig dienstverlening inzetten die security-dreigingen monitort. Dit Security Operation Center (SOC) fungeert eigenlijk als inbraakalarm: wanneer de dienst verdachte activiteiten op scholen detecteert, dan gaat de bel rinkelen. Denk aan dreigingen, mogelijke online aanvallen of data-inbreuk. Het geldt als eerste puzzelstukje in de strijd tegen cyber-criminaliteit in het onderwijs, en maakt scholen alerter. Toch is het niet genoeg.

Want gaat zo'n inbraakalarm af, dan wil je ook dat iemand kijkt wat er aan de hand is. Zelfs bij een vals alarm moet je zeker zijn. Is alles wel écht in de haak? Als de politie nooit komt kijken, is een alarm weinig zinvol. Dat geldt ook voor de SOC-dienst: na een melding is een goede reactie nóg belangrijker.

En dat is een uitdaging voor scholen, waar vaak kennis en mankracht ontbreekt om meldingen grondig te onderzoeken. Een willekeurige school met tienduizend leerlingen heeft duizend leerkrachten, en misschien maar tien ICT'ers. Dat staat niet in verhouding tot de gigantische, digitale footprint: er komen elke dag meer devices en cloud-platformen bij. Aanvallers hebben tal van ingangen en zijn vaak al binnen voor ze worden opgemerkt.

Dat ongelijke speelveld is deels op te vangen met een geïntegreerde omgeving. Als iets gedetecteerd wordt in een e-mail, dan kunnen ook de internetverbinding en endpoints worden gecheckt. Maar vaak zijn deze koppelingen niet aanwezig: leerlingen en studenten hebben een laptop, tablet, smartphone en allerlei online accounts. Hoe krijg je daar als school grip op? Adequaat *incident response* is dan het antwoord.

Pak security-incidenten aan voor het kwaad is geschied

Incident response is te vergelijken met een politieagent die langskomt als het alarm afgaat, maar het is tegelijkertijd een rechercheteam dat op onderzoek uitgaat. Een voorbeeld van incident response is Cisco Talos, een team security-experts dat ontwikkelingen op de voet volgt én bij veiligheidscalamiteiten orde op zaken stelt.

Met tooling controleert het team wat op dat moment in de getroffen IT-omgeving gebeurt. Sluizen applicaties data door? Zijn firewall-regels overschreden? Als de boosdoener gevonden is, wordt die onschadelijk gemaakt. Maar vervolgens is het belangrijk te weten hoe de inbreker is binnengekomen en waar schade is aangericht. Wellicht heeft een cyber-crimineel al beheerrechten gekregen en is de dreiging niet verdwenen.

Inzicht is fundamenteel. Daarom is acute hulp bij calamiteiten maar één onderdeel van incident response. Immers: als alarm wordt geslagen, is het leed vaak al geschied. Talos onderzoekt daarom ook mogelijke problemen. Is er al een slot gekraakt? Bij veel security-incidenten blijken aanvallers al lange tijd binnen te zijn, voor ze worden ontdekt. Dat risico is op scholen reëel, omdat het aanvalsoppervlak zo groot is.

Een goede voorbereiding is daarom het belangrijkst. De kans dat je alle aanvallen tegenhoudt is uitgesloten. Er moet daarom een draaiboek klaarliggen bij incidenten. Talos neemt scholen daarin mee en traint medewerkers. Door vooraf verschillende scenario's door te nemen, kent iedereen zijn rol bij een incident. Wanneer een school denkt dat het zijn zaken op orde heeft, checkt Talos met een *pentest* of dat écht zo is. Oftewel: zitten er genoeg sloten op de deur? Wat zijn de zwakke plekken? Hoe kunnen die versterkt worden?

Door beter in te zetten op incident response wordt het onderwijs veiliger. DVN brengt de security van scholen naar een hoger niveau. Niet alleen door in te grijpen bij noodgevallen, maar ook door te helpen bij de stappen die daarvoor én daarna volgen. Daarbij draait het niet alleen om de juiste security-oplossing, maar vooral om expertise. Je kunt een SOC hebben, mooie producten kopen en alles goed inrichten, maar zonder kennis heeft dat weinig zin. Talos helpt scholen op de juiste manier te reageren, en de cyberweerbaarheid van het onderwijs naar een hoger plan te tillen.