/// Kwetsbaarhedenbeheer

1 INTRODUCTIE

In uw organisatie gebruikt u veel verschillende IT-systemen en applicaties. In normale omstandigheden werken deze naar behoren, maar soms ook niet. Als deze IT-systemen en- applicaties niet op tijd gecorrigeerd of opgemerkt worden, kunnen cybercriminelen van deze situatie gebruik maken en hun slag slaan.

Om een dergelijk scenario te voorkomen, is het belangrijk om in uw organisatie een sterk kwetsbaarhedenbeheer te voeren. Dit zorgt er middels reviews, evaluaties en verificaties van systeemupdates, patches, kwetsbaarheidsscans en aanval- en penetratietesten voor dat kwetsbaarheden tijdig geïdentificeerd worden.

Om een succesvol beheer te implementeren is het ook belangrijk dat u het toezicht ervan toewijst aan een beleidsmedewerker. Deze persoon heeft dan de verantwoordelijkheid en bevoegdheid om de toepassing en naleving van het implementeren van het beleid op te volgen en eventuele inbreuken hiervan te rapporteren.

2 WET- EN REGELGEVING

Lokale besturen staan volgens de Belgische en Europese regelgeving vrij om hun kwetsbaarhedenbeheer in te vullen naar eigen behoefte.
Echter, lokale besturen dienen wel rekening te houden met de Algemene Verordening Gegevensbescherming (AVG) of GDPR (General Data Protection Regulation)[1]. Deze regelgeving schrijft voor dat alle bedrijven, overheidsdiensten, organisatie en instellingen die in Europa persoonsgegevens verwerken, gebruiken, registreren of bewaren, moeten voldoen aan bepaalde richtlijnen. Deze richtlijnen stellen dat gegevens volgens een afdoend veiligheidsniveau moeten worden verwerkt binnen een organisatie. Met andere woorden, om te voldoen aan de AVG wordt er verwacht dat persoonsgegevens niet zomaar door iedereen ingezien kunnen worden, en de systemen dus op een degelijke manier beveiligd zijn.

3 BELEID

Organisatorische maatregelen

Organisatorische maatregelen verwijzen naar het hebben van duidelijke processen, procedures en verantwoordelijkheden met betrekking tot kwetsbaarhedenbeheer. Bij het inrichten van kwetsbaarhedenprocedures is het belangrijk om te bepalen waar uw organisatie haar zwakke plekken zitten, en extra procedures voor deze zwaktes in te richten. Bijkomend is het belangrijk om de juistheid en

continuïteit van de beleidsprocedures en processen voor alle thema's die vallen onder kwetsbaarhedenbeheer periodiek te reviewen. Als er zich veranderingen voordoen in de organisatie, moet het management de opdracht geven om deze te integreren in het bestaande beleid. Tegelijk moet het management periodiek (externe) audits inplannen om het hele kwetsbaarhedenbeheer te controleren en om eventuele blinde vlekken te identificeren.

Technische maatregelen

Technische maatregelen verwijzen naar het hebben van documentatie waarin de werking, voorwaarden, verantwoordelijkheden en onderhoud met betrekking tot verschillende kwetsbaarhedenprocedures beschreven staan. Het wordt aangeraden om tenminste voor eindgebruikerbeveiliging, patchmanagement, aanvals- en penetratietesten en kwetsbaarhedenscans standaardprocedures te documenteren.

Mensgerichte maatregelen

Mensgerichte maatregelen verwijzen naar het hebben van bewustmakingscampagnes die het belang van eindgebruikerbeveiliging benadrukken bij gebruikers en applicatiebeheerders. Het is belangrijk om verantwoordelijkheden van eindgebruikers, zoals softwarerestricties, te communiceren naar hen.
Voor IT-medewerkers is het belangrijk om voldoende kennistrainingen te organiseren en het kwetsbaarhedenbeheer gebruiks- en onderhoudsvriendelijk houden.

4 AANBEVELINGEN

Hieronder vindt u een aantal aanbevelingen die het Cyber Response Team voor Lokale Besturen (Vo-CRT) geeft met betrekking tot de inrichting van een autorisatiebeheer.

Organisatorische maatregelen

- Zorg voor een actuele lijst van bedrijfsmiddelen waarvan kwetsbaarheden moeten worden opgevolgd.
- Zorg ervoor dat de verantwoordelijkheden rond het implementeren en onderhouden van kwetsbaarhedenbeheer processen en procedures goed gedefinieerd en bekend zijn.
- Zorg voor duidelijke afspraken rond het beheren van patchmanagement.
- Zorg ervoor dat het kwetsbaarhedenbeheer extra aandacht besteed aan de geïdentificeerde zwaktes of risico's binnen uw organisatie.
- Definieer voor het kwetsbaarhedenbeheer KPI's, en monitor en review deze op geplande tijdstippen.
- Voer regelmatig een audit uit die uw kwetsbaarhedenbeheer controleert.

Technische maatregelen

- Zorg ervoor dat de procedures en verantwoordelijkheden rond het uitvoeren en onderhouden van logging en alerting goed beschreven staan.

- Documenteer eventlogs en definieer hoe vaak logmaps gecontroleerd moeten worden.
- Zorg ervoor dat de procedures en verantwoordelijkheden voor het uitvoeren en onderhouden van patchmanagement goed beschreven staan.
- Gebruik een inventarisatielijst van IT-systemen en applicaties en definieer hoe vaak deze gescand moeten worden op gemiste updates.
- Zorg ervoor dat de procedures en verantwoordelijkheden voor het uitvoeren en onderhouden van aanvals- en penetratietesten goed beschreven staan.
- Bepaal hoe vaak en op welke manier netwerken blootgesteld moeten worden aan aanvals- en penetratietesten.
- Zorg ervoor dat de procedures en verantwoordelijkheden voor het uitvoeren en onderhouden van kwetsbaarhedenscans goed beschreven staan.
- Bepaal op welke termijn en door welke programma's interne en externe netwerken gescand moeten worden.
- Zorg voor een procedure die voorschrijft hoe nieuwe kwetsbaarheden het meest efficiënt behandeld kunnen worden.

Mensgerichte maatregelen

- Sensibiliseer medewerkers en beheerders over het belang van hun medewerking bij het domein eindgebruikerbeveiliging.
- Zorg ervoor dat in de onboarding van nieuwe medewerkers, het belang van kwetsbaarhedenbeheer benadrukt wordt.

5 VERKLARENDE WOORDENLIJST

Term	Verduidelijking	Link naar meer informatie
Eindgebruikerbeveiliging	Eindgebruikerbeveiliging verwijst naar de beveiligingprocedures die eindgebruikers in acht moeten nemen wanneer zij hardware- en software-activa gebruiken van een organisatie	Endpoint Protection Platform - Glossary | CSRC (nist.gov)
Logging en alerting	Logging en alerting verwijst naar het bijhouden van gebeurtenissen op hardware en software van een organisatie. Wanneer de gebeurtenissen afwijken van de standaard, wordt de beheerder van het logging- en alertingproces genotificeerd, en kan hij of zij actie ondernemen.	Guide to Computer Security Log Management | NIST
Patchmangement	Patchmanagement verwijst naar het verspreiden en in gang zetten van updates	Wat is Patch Management | IT Woordenboek | Marqit.be

	naar software. Dit is nodig om kwetsbaarheden of bugs te verhelpen in software.	
Aanvals- en penetratietesten	Aanvals- en penetratietesten verwijst naar een toets van een of meer computersystemen op kwetsbaarheden, waarbij deze kwetsbaarheden ook werkelijk gebruikt worden om in deze systemen in te breken.	Kwetsbaarheidsscan en testen van informatiebeveiliging | Vlaanderen Intern
Kwetsbaarhedenscans	Kwetsbaarheidsscans verwijst naar software die een overzicht van gedetecteerde kwetsbaarheden op de gescande systemen geeft.	Kwetsbaarheidsscan en testen van informatiebeveiliging | Vlaanderen Intern

REFERENTIES

- Kwetsbaarheidsscan en testen van informatiebeveiliging: Kwetsbaarheidsscan en testen van informatiebeveiliging | Vlaanderen Intern