Factsheet Patchmanagement

Bent u er zeker van dat al uw systemen volledig gepatcht zijn? Door achterstanden in updates kunnen er kwetsbaarheden zijn waar hackers misbruik van kunnen maken. Het proces waarmee beveiligingsupdates worden doorgevoerd noemen we patchmanagement. In deze factsheet wordt op hoofdlijnen ingegaan waarom patchmanagement essentieel is. Wat het doel ervan is. Hoe de CERT van de IBD hierbij kan helpen. Maar ook hoe u er zelf mee aan de slag kunt. Patchmanagement is één van de vier processen om de basisbeveiliging op orde te krijgen van het traject Verhogen Digitale Weerbaarheid Module 1.

Waarom patchmanagement essentieel is

Patchmanagement is van groot belang voor de beveiliging van de ICT-omgeving. Waar configuratiemanagement belangrijk is om te weten wat de gemeente in huis heeft, is het belang van patchmanagement om dat wat in huis is veilig te houden. Door tijdig te updaten en op structurele basis de juiste patches door te voeren kan worden voorkomen dat bekende kwetsbaarheden in software, hardware en besturingssystemen worden misbruikt. Kwetsbaarheden worden in toenemende mate geautomatiseerd misbruikt. Online scans vinden kwetsbare systemen en deze worden met behulp van eenvoudige tools geëxploiteerd. De gevolgen kunnen verstrekkend zijn voor de beschikbaarheid, integriteit en vertrouwelijkheid van systemen. Informatie kan worden gestolen, gewijzigd of versleuteld (ransomware), met alle financiële – en imagoschade van dien. Het is daarom zaak om een kwetsbaarheid zo snel mogelijk te verhelpen zodra een patch beschikbaar is gesteld. Het patchen van kritieke gekwalificeerde kwetsbaarheden ook verplicht vanuit de BIO (control 12.6.1). Kortom, patchen en updaten is van groot belang voor de informatiebeveiliging. Gemeenten kunnen door hun systemen up-to-date te houden veel grote en kleine incidenten voorkomen.

Wat is het doel van patchmanagement?

Het doel van Patchmanagement is tweeledig:

- het is gericht op het inzichtelijk maken van de actuele stand van kwetsbaarheden en toegepaste patches binnen de beheerde infrastructuur,
- op een zo efficiënt mogelijk wijze met zo min mogelijk verstoringen stabiele (veilige) systemen te creëren.

Patchmanagement en de IBD-CERT

De CERT van de Informatiebeveiligingsdienst (IBD) ondersteunt gemeenten met advies op het gebied van informatiebeveiliging en bij informatiebeveiligingsincidenten. Hieronder valt ook het versturen van kwetsbaarheidswaarschuwingen voor de nodige patches. De CERT baseert zich hierbij onder andere op de adviezen vanuit het Nationaal Cyber Security Centrum (NCSC). Het NCSC geeft beveiligingsadvies voor kwetsbaarheden in hard- en software. Zij bepalen aan de hand van impact en waarschijnlijkheid het risico dat een kwetsbaarheidswaarschuwing meekrijgt. Zij maken hiervoor gebruik van een internationale database voor kwetsbaarheden en vullen dit aan uit eigen bronnen. Veelal wordt een advies geschreven met de leverancier van het te patchen product. Al zijn er soms ook kwetsbaarheden bekend waarvoor de leverancier nog geen patch beschikbaar heeft gesteld. Na analyse zet de IBD dit opgestelde advies om in een advies voor gemeenten en verstuurt dit aan de relevante organisaties.
Het uitgangspunt is dat gemeenten weten wat zij in huis hebben (configuratiemanagement), de gemeente kan aan de IBD een ICT foto aanleveren die de basis vormt om de juiste kwetsbaarhedenberichten te ontvangen voor specifieke hard- en software. Zo kan de CERT passende kwetsbaarheidsmeldingen versturen voor alleen die software en hardware die relevant is. Het is dan wel essentieel dat deze ICT-foto actueel is, dat wil zeggen: dat de ICT-foto die componenten bevat waar u over gewaarschuwd wenst te worden.

Aan de slag!

Waar begin ik?

- Met configuratiemanagement zorgt u ervoor dat u inzicht heeft in welke software, hardware en besturingssystemen zich binnen de ICT-omgeving van de gemeente bevinden. Veelal is dit vastgelegd in een database (CMDB) en in een dossier met afspraken met leveranciers.
- Zorg voor een actuele ICT-foto. Zo ontvangt u tijdig relevante kwetsbaarheidsmeldingen. De IBD-CERT kan u helpen bij vragen hierover.
- Houd rekening met het onderscheid tussen reguliere patches en spoedpatches. Bij spoedpatches is de kans op misbruik hoog en is de mogelijke schade High/High (classificering NCSC). Deze patches dienen zo spoedig mogelijk te worden doorgevoerd, uiterlijk binnen één week (zoals de in BIO vastgelegd). Minder kritische beveiligings-updates/patches moeten worden ingepland bij de eerstvolgende onderhoudsronde van het systeem. Bij spoedpatches met de classificering High/High zal de IBD-CERT naast de reguliere waarschuwingen waar nodig ook een SMS versturen. Bij het ontvangen van een dergelijke SMS dient bij de gemeente direct het proces voor spoedpatches te worden ingezet. Waar nodig zal de IBD ook adviseren om het bestuur van de gemeente in te lichten over de situatie en de risico's.

Hoe begin ik?

- Goede afspraken zijn belangrijk. Waar worden kwetsbaarheidsmeldingen geregistreerd? Wie is verantwoordelijk voor het oppakken? Heeft de CISO een doorslaggevende rol in het proces? Leg dit vast of zorg voor een update van dat wat al voor het patchmanagement proces is vastgelegd. Zie ook de handreiking patchmanagement van de IBD voor meer ondersteuning hierop.
- Neem waar nodig mitigerende maatregelen als een belangrijke patch niet direct kan worden doorgevoerd. Plan vervolgens op korte termijn de patch in op een voor de bedrijfsvoering acceptabel moment. Advies hierover kan ingewonnen worden via de IBD-CERT.
- Leg afspraken voor patches vast in SLA's. Zo is ook het updaten bij leveranciers of ketenpartners geborgd.
- Controleer regelmatig op relevante patches en recente meldingen vanuit de IBD CERT.
- Leg toegepaste patches vast in bijv. het CMDB voor een overzicht van welke hardware, software en besturingssystemen up-to-date zijn en welke (nog) niet.

Hoe pak ik het structureel op?

- Zorg ervoor dat patchmanagement is vastgelegd in duidelijke afspraken en procedures. Dit hoeft niet veel tekst te zijn. Er dient minimaal bepaald te zijn wie waarvoor verantwoordelijk is en hoe applicatiebeheerders testen of de patch is geslaagd en de dienstverlening niet onacceptabel wordt verstoord. In de handreiking patchmanagement is hiervoor vanuit de IBD ook een patchmanagementbeleid en een mogelijke procesbeschrijving uitgewerkt. Denk hierbij ook aan afspraken over (financiële-) middelen als bijvoorbeeld overwerken buiten reguliere kantoortijden en eventuele inhuur van derden.
- Controleer minimaal jaarlijks of het patchmanagementproces actueel en beschreven is en of verantwoordelijkheden juist zijn belegd. Zo kunnen misverstanden worden voorkomen en worden patches tijdig doorgevoerd en daarmee kwetsbaarheden gedicht.
- Borg in techniek, maar ook in het risicomanagement proces en beveiligingsbewustzijn dat updates niet te lang worden uitgesteld.

De basis op orde en klaar voor de volgende stap?

- Door overbodige software, services en gebruikersaccounts uit te schakelen en/of van de systemen te verwijderen kunnen de aanvalsmogelijkheden op het systeem worden verkleind en nemen de risico's op achterstallige patches af. Dit proces wordt ook wel hardening genoemd. Meer hierover is verder uitgewerkt in het hardening beleid voor gemeenten.
- Speciale tooling kan het patchmanagement proces ondersteunen. Denk hierbij aan vulnerability scanningtools die actief zoeken naar kwetsbaarheden binnen het netwerk.
- Het laten uitvoeren van een penetratietest kan kwetsbare systemen blootleggen die gepatcht dienen te worden. Daarbij kunnen ook systemen meegenomen worden die buiten beeld zijn geraakt of gebruik maken van verouderde techniek, waar hackers misbruik van kunnen maken. Het is dus van groot belang dat ook deze systemen worden opgespoord en worden afgedekt doormiddel van updates of mitigerende maatregelen.
- Zorg voor een test/acceptatie-omgeving zodat patches niet in de productieomgeving getest hoeven te worden met mogelijke negatieve gevolgen voor de dienstverlening. Dit kan heel goed een onderdeel zijn van het changemanagement proces van de gemeente.

Tips uit de praktijk

- Sommige gemeenten kiezen ervoor om de kwetsbaarheidsmeldingen te registreren in hun ITIL ticketsysteem of spelen het door aan de ICT-Servicedesk. Zo kan de registratie worden vastgelegd en dient binnen de afgesproken SLA vanuit de servicedesk een actie te volgen. Daarbij is het zaak dat ook de CISO tijdig van de kwetsbaarheidsmelding op de hoogte wordt gesteld om hierbij een risicoschatting voor het patchen te maken. Dit heeft een rechtstreekse relatie met het change management proces van de gemeente.
- Start een mail-, Whatsapp- of Signal-groep waar de functies en personen in zitten die direct op de hoogte moeten worden gesteld in het geval van een kritische kwetsbaarheid. Zo is er direct afstemming voor een risicoschatting en het bepalen van vervolgacties. Ook kan dan snel besloten worden of verdere afstemming noodzakelijk is om de dreiging te mitigeren.
- Evalueer en leer. Gaf een eerdere patch problemen? Of liet een update langer op zich wachten dan de afspraak? Ga na hoe dit in de toekomst beter kan.

Waar vind ik meer?

Verhogen Digitale Weerbaarheid Module 1
https://www.informatiebeveiligingsdienst.nl/project/digitaleweerbaarheid/ inclusief de mindmap processen.

Handreiking patchmanagement voor gemeenten BIO
https://www.informatiebeveiligingsdienst.nl/product/patch-management-voor-gemeenten/

Handreiking Hardening-beleid voor gemeenten
https://www.informatiebeveiligingsdienst.nl/product/hardening-beleid-voor-gemeenten/

Handreiking penetratietesten BIO
https://www.informatiebeveiligingsdienst.nl/product/handreiking-penetratietesten/

Baseline Informatiebeveiliging Overheid (BIO)
https://www.informatiebeveiligingsdienst.nl/product/baseline-informatiebeveiliging-overheid-bio/

Kijk voor meer ook op de productenpagina van de IBD;
https://www.informatiebeveiligingsdienst.nl/kennisproducten-ibd/

U kunt de IBD altijd om advies vragen.

Meer informatie

Meer informatie over onze dienstverlening vindt u in de andere factsheets van de IBD en op de website www.informatiebeveiligingsdienst.nl. De helpdesk van de IBD is te bereiken tijdens kantooruren van 9:00 tot 17:00 uur op het nummer 070 204 55 11 of via het e-mailadres info@IBDgemeenten.nl. De CERT van de IBD is 24x7 bereikbaar via 070 204 55 11 (instructies voor het piketnummer op de voicemail).