Veiligheidsregio Noord- en Oost Gelderland
De heer H. Damen
Europaweg 79
7336 AK APELDOORN

Voortgangsrapportage

Voortgangsrapport

Datum: 31-10-2014	Tijd: 23:30
Betreft: Escalatie VNOG dd. 31	

Coördinatoren: Marcel Janssen (IT-Value) Hans Damen (VNOG)	**Datum Rapportage:** 31-10-2014	

Tijdslijn:

31-10-2014 – 15:00
IT-Value aangekomen bij VNOG voor uitvoering van mitigerende maatregelen.
Aanwezigen bij het voor overleg zijn:

- Hans Damen (VNOG)
- Gerry van Cleef (VNOG)
- Wim <achternaam onbekend> (VNOG)
- Sander Daems (IT-Value)
- Marcel Janssen (IT-Value)

31-10-2014 – 15:15
Vaststelling van prioriteiten van de door IT-Value beschreven maatregelen in overleg met VNOG

31-10-2014 – 15:45
De volgende maatregelen zijn door VNOG en IT-Value benoemd met de hoogste prioriteit en derhalve direct door te voeren. Deze zijn:

#	Actie	Prioriteit	Uitvoerende partij
1	Alle Domains Admin accounts binnen het VNOG netwerk aanpassen	Hoog	VNOG / IT-Value
2	VPN user accounts identificeren en wachtwoorden wijzigen	Hoog	VNOG / IT-Value
3	Firewall (Juniper) en TMG logs veiligstellen voor nader onderzoek	Hoog	VNOG / IT-Value
4	VPN Logs analyseren op inkomende verbindingen tussen 25 oktober en 31 oktober	Hoog	VNOG / IT-Value

5	Active Directory groepen controleren op lidmaatschap incl. Nested Groups	Hoog	VNOG / IT-Value
6	Administrator wachtwoorden aanpassen op kritische netwerk en internet facing componenten zijnde: - Core Switches - Netscalers - Ironport - Firewalls (Juniper/TMG) - Citrix Sharefile	Hoog	VNOG / IT-Value
7	Virusscans over alle systemen binnen het VNOG netwerk	Hoog	VNOG / IT-Value
8	Controleren of en welke user objecten sinds 25 oktober in Active Directory zijn aangemaakt en aangepast	Hoog	VNOG / IT-Value
9	Change log van TMG doornemen op onregelmatigheden zoals: - Zijn er policies aangemaakt - Zijn er rules aangemaakt of gewijzigd - Zijn er users aangemaakt of gewijzigd	Hoog	VNOG / IT-Value

Op basis van de analyse en resultaten van de door IT-Value aangeboden Security Audit worden door VNOG en IT-Value vervolgstappen besproken.

31-10-2014 - 16:00 uur:
Gestart met uitvoer van de bovengenoemde acties door IT-Value en VNOG Door:
Hans Damen (VNOG)
Wim (achternaam?) (VNOG)
Sanders Daems (IT-Value)

31-10-2014 – 18:15 uur:
Uit te voeren acties afgerond. Hieronder volgende de resultaten van de 8 beschreven acties:

1) **Alle Domains Admin accounts binnen het VNOG netwerk aanpassen:**
   Adm-Accounts van Servicedesk disabled, mail gestuurd naar de medewerkers dat de wachtwoorden maandag worden aangepast. Overige Domain admin accounts wachtwoorden gewijzigd of accounts disabled. De volgende accounts zijn disabled:
   - Adm-decos disabled (leveranciers account)
   - Adm-johan; Gechecked staat op disabled
   - Adm-nick: Gechecked staat op disabled.

2) **VPN user accounts identificeren en wachtwoorden wijzigen:**
   Er zijn op dit moment 3 VPN users actief namelijk: Gerry, Hans en Gerard.
   Wachtwoorden van alle 3 accounts zijn aangepast.

3) **Firewall (Juniper) en TMG logs veiligstellen voor nader onderzoek**
   Juniper logs veilig gesteld voor verdere analyse
   Er is geconstateerd dat de TMG firewall geen logging heeft Hierdoor geen logging veilig kunnen stellen voor dit component.

4) **VPN Logs analyseren op inkomende verbindingen tussen 25 oktober en 31 oktober:**
VPN is geconfigureerd op de TMG Firewall. De TMG firewall heeft geen logging aan staan. Hierdoor is het niet mogelijk mogelijke inbound connecties via VPN te detecteren.

5) **Active Directory groepen controleren op lidmaatschap incl. Nested Groups**
Domain admin groep gecontroleerd. De volgende domain admin accounts vereisen nader onderzoek. Hiervan is niet duidelijk waarom ze nog lid zijn van de domain admins groep. De accounts zijn wel herkenbaar maar betreffen oude VNOG systemen.
- Svc.dpm
- Svc.hpdp6
- Svc.mcafee
- Svc.sccm2007
- Svc.sccm2007naa
- Svc.Scom2007aa
- Svc.Scom2007dw
- Svc.Scom2007sdk
- Svc.Scom2007.ad

VNOG gaat de bovengenoemde accounts controleren op juistheid en waar mogelijk disablen en verwijderen uit de Domain Admins groep
Enterprise Admins, OK bevonden, geen vreemde accounts gevonden
Schema Admins --> OK bevonden, geen vreemde accounts gevonden
Domain Computers --> OK bevonden, geen vreemde accounts gevonden
Exchange Organization Admins --> OK bevonden, geen vreemde accounts gevonden
Recipients Admin --> OK bevonden, geen vreemde accounts gevonden

6) **Administrator wachtwoorden aanpassen op kritische netwerk en internet facing componenten zijnde:**
- Core Switches: Wachtwoorden van privileged accounts op beide core switches aangepast;
- Netscaler: Wachtwoorden Local administrator accounts op de Netscaler aangepast
- Ironport: Wachtwoorden Privileged accounts aangepast
- Firewalls (Juniper/TMG): Wachtwoorden lokale accounts aangepast
- Citrix Sharefile: Wachtwoorden lokale accounts aangepast

7) **Virusscans over alle systemen binnen het VNOG netwerk**
Constatering: Niet alle Servers zijn bekend binnen Symantec. Voor alle binnen Symantec bekende systemen is een Full System scan gestart. VNOG controleert de resultaten van de scans a.s. maandag 3 oktober

8) **Controleren of en welke user objecten sinds 25 oktober zijn aangemaakt en aangepast**
Powershell script gemaakt en uitgevoerd op beide domain controllers voor het controleren van aangemaakte en gewijzigde user objecten sinds 25 oktober. De gebruikte filters zijn:

- User Objecten
- Modified en Created
- Sinds 25 oktober 2014

Er zijn geen onregelmatigheden geconstateerd in de aanmaak en het wijzigen van de user objecten in de genoemde periode

9) Change log van TMG doornemen op onregelmatigheden zoals:
Sinds 21 oktober 2014 zijn er op de TMG geen wijzigingen meer doorgevoerd. De laatste wijziging op 21 oktober 2014 is gedaan door adm.wim

Naast de vastgestelde acties is tevens vastgesteld dat:
- Er in de periode 25 oktober tot nu geen security events zijn geconstateerd die te herleiden zijn naar dit incident
- Er zijn geen installaties of wijzigingen uitgevoerd op de Domain Controllers

Vervolg stappen:

- Maandag 03 oktober wordt een security audit uitgevoerd door een onafhankelijke partij (On2IT);
- IT-Value is maandag 03 oktober aanwezig voor technische ondersteuning en aanvulling voor het uitvoeren van vervolg acties bijvoorbeeld het controleren van de Full-System scan van Symantec
- Na uitvoering van de security audit wordt het rapport en de aanbevelingen besproken en worden eventuele vervolgstappen besproken tussen IT-Value en VNOG

Volgende voortgangsrapportage:
- Dinsdag 04 oktober