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

Escalatie rapportage

Escalatierapport

Opening	Datum: 25-10-2014	Tijd: 13:10
Afsluiting	Datum: 31-10-2014	Tijd: 10:03

Melding ontvangen via: VNOG

Omschrijving storing:

- FTP server aangetroffen met netwerkdocumentatie over de VNOG.
- Op de server stond tevens een txt bestand met wachtwoorden die bestemd waren voor IT-Value 24 x 7 dienstverlening.
- FTP server was vrij toegankelijk, zonder gebruikersnaam & wachtwoord validatie.
- FTP adres ftp://159.253.7.166/CloudUsr001/

Impact: Nader te bepalen

Geëscaleerd bij:	**Datum/tijd escalatie:**	**Datum/tijd afmelding:**
Maurice Aalders	31-10-2014	Gesloten

Tijdslijn:

Nav de geconstateerde openstaande FTP server is onderzocht wanneer en dus hoelang de informatie beschikbaar geweest is. De hierna volgende tijdslijnen geven het verloop van feiten weer:

25-10-2014 – 13:10 uur:
IT-Value heeft de data geplaatst op FTP server opdat 24x7 partner de data over kan nemen voor de dienst beveiligd met user en wachtwoord en verstuurd naar partner.

30-10-2014 – 20:18 uur:
VNOG ontvangt melding van MathijnvanBeest@ibix.nl. Martijn heeft geconstateerd dat de gevoelige informatie vrij toegankelijk beschikbaar is op een FTP server

31-10-2014 – 09:18 uur:
VNOG informeert IT-Value over de beschikbaarheid van de data en vraagt opheldering.

31-10-2014 – 09:30 uur
Onderzoek gestart naar afkomst server. Afkomst FTP server geïdentificeerd.

31-10-2014 – 10:03 uur:
Data is verwijderd van de FTP Server / Internet tevens is de server off-line gebracht.

31-10-2014 – 10:15 uur:
Onderzoek naar oorzaak toegankelijkheid ftp server zonder wachtwoord.

31-10-2014 – 11:00 uur:
FTP directory listing configuratie blijkt onjuist. De directorie structuur en bestanden waren hierdoor voor "anonymous-users" zichtbaar.

31-10-2014 – 11:45 uur:
Gedurende de periode dat de data beschikbaar was op de FTP server zijn 5 verbindigen tot stand gekomen:
Log xferlog: CloudUsr001 met VNOG data (zie bijlage 2)

- Mon Oct 27 14:23:07 2014 1 62.58.0.74 = diabolo
- Mon Oct 27 18:36:27 2014 3 113.161.75.183 <-- AZIE, zie arin.net
- Thu Oct 30 19:20:13 2014 1 77.173.121.156 <-- moet dan de melder zijn Mathijn van Beest, wellicht kunnen wij dit navragen
- Fri Oct 31 08:56:13 2014 1 195.7.142.66 = VNOG
- Fri Oct 31 09:32:47 2014 1 145.131.138.169 = IT-Value

Oorzaak van storing:
IT-Value werkt samen met een IT-Partner voor het leveren van de 24x7 dienstverlening. Om ten tijde van een calamiteit goed te kunnen acteren is het noodzakelijk de documentatie & inlog gegevens te delen met de partner.
Vanwege de omvang van de totale beschikbare documenten is gekozen voor een FTP uitwisseling. In de uitwisseling van de FTP server gegevens naar de partner toe is te zien dat een gebruikersnaam en wachtwoord geactiveerd waren;
ftp://CloudUxr001:J7kl3zNNQB@159.253.7.166

Uit de URL is op te maken dat gebruik is gemaakt van een gebruikersnaam & wachtwoord.
Username: CloudUsr001
Wachtwoord J7kl3zNNQB
IP adres 159.253.7.166

Oplossing:

- De data is verwijderd van de FTP Server en de FTP server is uitgezet.
- Overige stappen ter voorkoming van, maar zeer zeker ook ter validatie van de omvang van het incident, zijn onder het hoofdstuk risico's & acties opgenomen.

Risico's voor VNOG:

- Het account & wachtwoord dat te downloaden was, was een account op het hoogste niveau binnen de Active Directory repository (AD is de opslag locatie van alle accounts van de VNOG).
- Het account is in principe bruikbaar geweest voor de buitenwereld, echter enkel een account, zonder informatie van servers en / of het netwerk is een beperking voor het verkrijgen van verdere toegang.

- De FTP server geeft aan dat een 5-tal verbindingen zijn opgezet naar de FTP server. 5 potentiele gebruikers die de beschikking kunnen hebben over de gegevens.

Acties om de impact van de verstoring te beperken:
Ter voorkoming van eventueel misbruik is het noodzakelijk de wachtwoorden van belangrijke componenten (Admin accounts, switches, firewall, VPN tunnels) direct aan te passen.

IT-Value adviseert de hierna volgende acties z.s.m. moeten worden uitgevoerd;
IT-Value stelt per direct vandaag, zijnde 31-10-2014 ter ondersteuning cq uitvoering van de acties, een consultant en een incident coordinator beschikaar (operationeel manager).

#	Actie	Prioriteit	Uitvoerende partij
1	Alle Domains Admin accounts binnen het VNOG netwerk aanpassen	Hoog	VNOG / IT-Value
2	Alle switches nalopen en wachtwoorden wijzigen van deze switches	Hoog	VNOG / IT-Value
3	PPTP VPN logs nalopen	Hoog	VNOG / IT-Value
4	Active Directory groepen controleren op lidmaatschap incl. Nested Groups	Hoog	VNOG / IT-Value
5	Alle accounts die in de VNOG KeePass staan nalopen en wachtwoord aanpassen	Hoog	VNOG / IT-Value
5a	Service accounts wachtwoorden aanpassen	Hoog	VNOG / IT-Value
6	Met policy Local Administrator wachtwoorden aanpassen	Hoog	VNOG / IT-Value
7	Virusscans over alle systemen binnen het VNOG netwerk	Hoog	VNOG / IT-Value
8	krbtgt account wachtwoord aanpassen	Hoog	VNOG / IT-Value
9	SQL & Applicatie servers nalopen op extra accounts / recent gewijzigde account	Hoog	VNOG / IT-Value
10	Logs Extern -> Intern nalopen	Hoog	externe security audit
a	Citrix Sharefile logs nalopen	Hoog	externe security audit
B	Outlook Web App nalopen	Hoog	externe security audit
C	Firewall logs nalopen	Hoog	externe security audit
D	TMG logs nalopen	Hoog	externe security audit
e	Netscaler logs nalopen	Hoog	externe security audit

In de bijlage is een detaillering opgenomen van de uit te voeren acties.

Extra tegenmaatregel:

Zoals de actielijst beschrijft stelt IT-Value voor een security specialist in te schakelen ter validatie van het voorval en ter bevestiging van de veiligheidssituatie nu.
Bijlage:  20141031 Stappenplan escalat