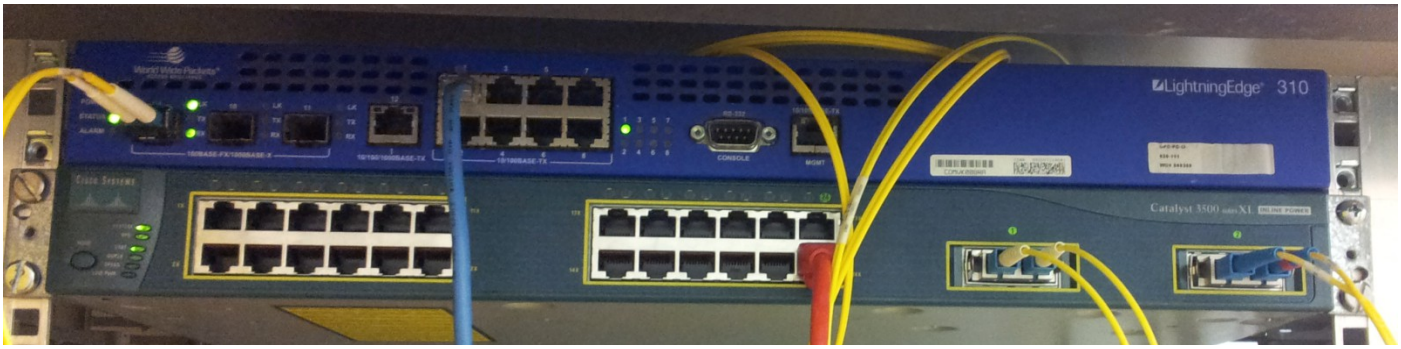
Nadat een computervereniging (Nurdspace) intrek had genomen in een oud gebouw, was men bezig om te kijken naar de mogelijkheden om een internetverbinding op deze locatie te krijgen. Het oude schoolgebouw had alleen zeer slechte mogelijkheden om een internet aansluiting te realiseren en de hoop was een fiber te vinden die in de buurt van bestaande fiber-infra uitkomt. Op deze manier was het de bedoeling om voor een zachte prijs toch een fatsoenlijke internetverbinding op de locatie te krijgen. Tijdens de speurtochten door het grote gebouw is een aantal fibers aangetroffen waarvan er nog een actief was.

Op 24 juli 2013 ben ik begonnen om uit te zoeken wat die vezel nu precies deed. Omdat de kabel niet gelabeld was konden we niet makkelijk achterhalen van welke provider deze verbinding was om ze te benaderen of we daar gebruik van konden maken. De enige manier om daar achter te komen was het werkend krijgen van de verbinding en te kijken wat voor verkeer er zichtbaar was.



Eerst moesten we achterhalen welke hardware we hiervoor nodig hadden. Na het meten van de vezel bleek dat deze ~3km was, en na een 'splitter' erop te hebben gezet bleek dat het 1310nm betrof. Na wat benodigde apparatuur bij elkaar te hebben gesprokkeld en aangesloten kregen we ook netjes een link.

Uit de fiber zagen we twee soorten verkeer binnen komen, namelijk een VLAN 127 die gebruikt werd voor het beheer van de CPE, en een VLAN 128 waar middels Q-in-Q de VLAN's van de klant in gezet werden. Bij het dumpen van VLAN 127 werd duidelijk dat dit om een KPN fiberverbinding ging, omdat de benamingen daarop duidden.

No.	Time	Source	Destination	Protocol	Length	Info
2	0.016688	10.93.143.253	224.0.0.18	VRRP	60	Announcement (v2)
6	1.016784	10.93.143.253	224.0.0.18	VRRP	60	Announcement (v2)
11	1.481167	AlcatelN_13:4a:ab	Broadcast	ARP	64	Who has 10.93.139.81? Tell 10.93.143.253
12	1.481283	AlcatelN_13:4a:ab	Broadcast	ARP	64	Who has 10.93.139.169? Tell 10.93.143.253
13	1.481371	AlcatelN_13:4a:ab	Broadcast	ARP	64	Who has 10.93.139.165? Tell 10.93.143.253
17	2.016692	10.93.143.253	224.0.0.18	VRRP	60	Announcement (v2)

Na het aansluiten van een laptop en het configureren van de switch voor VLAN 127 kreeg de laptop vanaf een DHCP-server meteen interessante informatie. De vezel kwam uit in de KPN centrale in Wageningen op een Alcatel 'Ethernet Service Switch' op poort 1/06 en de CPE zou daarbij de volgende opties krijgen:

Fixed – Address	10.93.131.193
Filename	/wwp/le310/le-4xx3xx.xml
Server-name	10.37.7.14
Option netmask	255.255.240.0
Option time-offset	7200
Option routers	10.93.143.254
Option dhcp-lease-time	691200
Option tftp-server-name	10.37.7.15
Option time-servers	10.37.7.2, 10.37.7.130
Option bootfile-name	/wwp/le310/le-4xx3xx.xml
Option dhcp-message-type	5
Option dhcp-server-identifier	10.37.7.14
Option dhcp-renewal-time	86400
Option dhcp-rebinding-time	172800
Option dhcp-name	NL-WG-P106-NGEK-310-01

De CPE's die KPN hiervoor gebruikt zijn o.a. de WWE LightningEdge 310. We hebben deze via-via op de kop getikt en achter onze switch erbij gehangen. Op die manier konden we zowel voor als achter de CPE het verkeer zien. Daarbij viel op dat VLAN 127 door de CPE gestript werd en niet doorgezet werd naar de beschikbare ethernet poorten.

Het mooie van deze constructie was dat we zowel de verbinding online hadden met de CPE zoals dat origineel moet werken, maar met de switch die ertussen zat ook toegang tot VLAN 127 mogelijk bleef. KPN ziet aan hun kant dus niets anders dan een werkende verbinding. Alle CPE's lijken dusdanig geconfigureerd dat ze vrij uitwisselbaar zijn. Dat was ook te zien aan de standaard configuratie die de CPE mocht ophalen:

```
aggregation set port 1-8,11-12 agg-mode manual
vlan add vlan 127 port agg1
vlan remove vlan 1 port agg1
vlan remove vlan 127 port 1-8,10-12
```

Verder konden we uit de CPE configuratie opmaken dat er nog twee managementnetwerken zijn: 172.16.233.0/24 en 10.37.199.0/24 en dat er twee radius-servers zijn voor authenticatie, namelijk 10.37.7.5 en 10.37.7.15. Daar hebben we destijds niet verder naar gekeken en nadat de verbinding afgesloten was, was dat ook niet meer mogelijk. Mogelijk dat er in die netwerken nog meer interessante informatie te verzamelen was.

Na de TCPdump een paar uur lang gedraaid te hebben en deze informatie te hebben geanalyseerd wisten we dat:

- Achter elke vezel kan slechts 1 MAC-adres een IP via DHCP krijgen in VLAN 127. Dat IP behoort te leven op de CPE ten behoeve van het beheer. Het MAC adres wordt voor 14 dagen onthouden, dus de CPE moet minimaal 14 dagen offline zijn om met een ander apparaat op de verbinding een IP-adres te krijgen en het netwerk in te kunnen. Handmatig een IP-adres pakken in dezelfde range functioneerde op dat moment ook niet. We moesten vanaf dat moment het MAC adres klonen om gebruik te blijven maken van het IP op verschillende machines.

- Het management-VLAN naar de CPE was beperkt tot een snelheid van 256KB/s.

- De IP-range waar de CPE in stond leek specifiek voor de regio. Het CPE kreeg ook een default gateway waarmee je dieper het KPN-netwerk in kon. Deze router had wel specifieke routes staan voor het CPE bronnetwerk, sommige ranges waren dus niet rechtstreeks bereikbaar vanuit de CPE zonder daar handmatig wijzigingen in te maken.

- De IP-range (10.37.7.0/24) waaruit de DHCP uitgegeven werd was dezelfde waaruit beheer werd gedaan en had o.a. DNS, tFTP, FTP en wat managementservers.

- Er was een aantal community strings (zelfs 'WRITE' community strings) die op “onze” vezel binnenkwamen a-la-broadcast terwijl zowel de SRC als DST niet achter die vezel bestond. Dat SNMP verkeer zou er niet binnen moeten komen, maar was met regelmaat duidelijk te zien in de TCPdumps:

  158170 22761.385301 10.37.7.130 10.93.131.3 SNMP 153
  get-request 1.3.6.1.2.1.2.2.1.7.1 1.3.6.1.2.1.2.2.1.8.1 1.3.6.1.2.1.31.1.1.1.1.1 1.3.6.1.2.1.2.1.0
  Community : xxxxxxxxxxxxxx Version 1

Nu was het doel niet om ernaar te kijken, maar het was nu dusdanig interessant om eens een korte blik te werpen in de gevonden management -IP-space. Met een NMAP van het netblock is weer wat interessant informatie gevonden:

- Op een tweetal IP-adressen draaide een nameserver die volledige recursing was (ook leuk voor DNS amplification attacks), maar ook gewoon AXFR ondersteunde mits je de naam van de zone weet. Deze naam werd bijgesloten in de DHCP-reply dus het was kinderspel geweest om een volledige lijst van routers, hun IP, en KPN benaming te downloaden wat met een CNAME naar de CPE verwees:

  ; <<>> DiG 9.8.1-P1 <<>> @10.37.7.2 connect axfr
  ; (1 server found)
  ;; global options: +cmd
  connect. 86400 IN SOA ogma.connect. root.ogma.connect. 2013073402 10800 3600 604800 86400
  connect. 86400 IN NS ogma.connect.
  ...

  nl-asd-p9450-ngek-310-01-lo0.connect. 86400 IN A 10.93.15.69

  nl-asd-p9451-ngek-310-01.connect. 86400 IN CNAME nl-asd-p9451-ngek-310-01-lo0.connect.

  nl-asd-p9451-ngek-310-01-lo0.connect. 86400 IN A 10.93.14.236

  nl-asd-p9455-ngek-310-01.connect. 86400 IN CNAME nl-asd-p9455-ngek-310-01-lo0.connect.

  ...

  netcios2.connect. 86400 IN A 10.37.7.38

  netcios3.connect. 86400 IN A 10.37.7.39

  ogma.connect. 86400 IN CNAME ogma-mgmt.connect.

  ogma-bck.connect. 86400 IN A 10.64.124.55

  ogma-mgmt.connect. 86400 IN A 10.37.7.34

  ogma-rib.connect. 86400 IN A 10.32.6.126

  ogma-trf.connect. 86400 IN A 10.37.7.2

  …

- Een aantal IP-adressen was overduidelijk bestemd voor verbindingen naar o.a. de CPE’s om ze te beheren.

- Het IP 10.37.7.2 had een FTP server draaien. Een poging om te verbinden naar de FTP lukte niet alleen, maar was mogelijk met de 'anonymous' account! Deze server is voor analyse (en PoC) verzameld en bevatte ruim 1000 configuratiebestanden voor routers, switches en andere apparaten:

  10.50.168.1-confg
  apel-p14-msad-01-confg
  ww-p74-msad-01-confg
  ...

Die avond heb ik een aantal van deze configs bekeken, en wat bleek: een groot aantal Cisco apparaten had een 'password type 7 $crypto_pass' dat simpelweg (in seconden) te reverse-engineeren is. De meeste apparaten hebben wel een ACL zodat je enkel vanuit het IP-segment voor beheer kunt verbinden:

172.16.25.166 nl-ah-c-mipc-cr02-confg:	neighbor 62.133.125.128 password xxxxxxxxxxxxx
172.16.25.166 nl-ah-c-mipc-cr02-confg:	password xxxxxxxxxxxxx
172.16.25.166 nl-ah-c-mtib-cr02-confg:	neighbor 139.156.118.1 password xxxxxxxxxxxxx
10.50.45.9 nl-asd-2-gmn-ax99-confg:	password xxxxxxxxxxxxx
10.77.20.36 nl-gv-dc2-mtib-cr01-confg:	password xxxxxxxxxxxxx
10.50.2.243 nl-hd-c-gmn-ar01-confg:	neighbor 10.50.3.100 password xxxxxxxxxxxxx
10.50.0.100 nl-mt-c-lbns-ar01-confg:	password xxxxxxxxxxxxx
set system -readCommunity	xxxxxxxxxxxxx
set system –writeCommunity	xxxxxxxxxxxxxnl-nd-c-gmn-ax02-confg:
enable secret 5 xxxxxxxxxxxxx	

Na een uurtje of twee rondkijken was duidelijk dat er dusdanige toegang mogelijk was tot het interne netwerk van KPN dat een kwaadwillend persoon flinke schade zou kunnen toebrengen aan de KPN-infra. Ik zie mijzelf totaal niet als een hacker en denk dat een goede hacker hier zeker meer had kunnen vinden, bijvoorbeeld een manier kunnen vinden om de ACL te omzeilen door het hacken van de FTP server omdat deze voor een verouderde machine nog flink open stond. Omdat de mogelijkheden van de aangetroffen situatie dermate ernstig was hebben we de zoektocht naar een internetverbinding gestaakt en de informatie verzameld om er melding van te gaan maken.

De volgende dag heb ik via connecties bij het NCSC een anonieme melding laten doen bij KPN. Om aan te tonen dat ik toegang had verkregen tot bepaalde zaken had ik de decrypted passwords inclusief routernamen doorgegeven. Het NCSC had op haar beurt weer goede contacten met KPN-CERT en hadden vrij snel een reactie ‘oh crap’, gevolgd door het verzoek om in contact konden komen met de melder om deze wat vragen te stellen. Mijn (vooral negatieve) ervaringen van KPN uit het verleden weerhield me enigszins, maar heb ik uiteindelijk toch besloten rechtstreeks contact op te nemen met KPN-CERT om gegevens uit te wisselen over het lek.

Vervolgens is het KPN-CERT er mee aan de slag gegaan en de contacten die ik met dat team heb gehad waren tot mijn verbazing erg goed. Na een paar dagen, diverse gesprekken en een bezoek op de locatie waar de 'testopstelling' stond was duidelijk dat het een serieuze zaak betrof en werd er zelfs meer gevonden door KPN dan ik zelf tot zover al had aangetroffen. Tijdens hun bezoek heb ik KPN onze verzameling aan data (TCPdumps, FTP server dump, DNS zone dump, etc) meegeven zodat ze daar eventueel nog meer informatie uit konden halen.

Na de melding heeft een gespecialiseerde afdeling binnen KPN (het 'RED-team') verder onderzoek gedaan wat mogelijk zou zijn met de verkregen informatie en heeft men naast de gevonden problemen nog andere problemen geconstateerd die zeker aandacht nodig hadden. Inmiddels heeft KPN de meeste zaken opgelost en is een dergelijke toegang ook niet meer mogelijk.

Helaas heeft KPN de glasvezel laten afsluiten zodat we nu helemaal geen werkende verbinding meer hebben en aanvragen van een nieuwe (betaalbare) verbinding was, ondanks de poging die de KPN-CERT medewerkers voor ons gedaan hebben, vooralsnog niet mogelijk geweest. Daarmee ligt een prima werkende internetverbinding zijn laatste dagen te verstoffen tot het pand tegen de vlakte gaat, wat erg jammer is.

Nu steeds meer bedrijven het nut zien om een Responsabele Disclosure-policy op te stellen en daarmee de drempel voor het melden van lekken flink verlagen zal het dergelijke bedrijven op de langere termijn alleen maar baten. Het is natuurlijk nooit leuk om te horen dat er een lek is, maar dat je een melding krijgt van een lek, en dat daar geen misbruik van gemaakt werd door de melder, kan dat het bedrijf een flinke schade schelen. De (White-hat) hackers die het leuk vinden om zulke zaken te vinden krijgen dan ook meer ruimte om zich door bepaalde systemen te wurmen.

Ook de rol van het NCSC is hier niet onbelangrijk in geweest, omdat het hackers toelaat om een melding te laten doen naar het gehackte bedrijf zonder dat direct mijn persoonsgegevens bekend gemaakt worden. Daarbij heeft het NCSC veel connecties en kan daarmee zorgen dat een melding snel op de juiste plaats komt en serieus genomen wordt.

Helaas is het ethisch hacken, ondanks het een correct melden ervan, veelal nog steeds een strafbaar feit. Je hebt je immers toegang verschaft op een manier die niet toelaatbaar is. Het melden van een lek zal in 99,9% van de gevallen goed aflopen, maar als het bedrijf of openbaar ministerie er toch een zaak van besluit maken moet je maar hopen dat het goed afloopt. De wet loopt zoals gewoonlijk achter de feiten aan, maar het zou haar sieren om in dit digitale tijdperk een voorziening te treffen om ‘digitale klokkenluiders’ (mits men geen misbruik ervan maakt) te beschermen tegen vervolging. Ik kan mij namelijk prima voorstellen dat het sommige personen ervan weerhoudt om melding te maken van een lek, omdat ze bang zijn voor een mogelijke aangifte.