Dacht je dat je 'hack-proof' was!

Ruud Uphoff

Soms denk je alle mogelijke veiligheidsmaatregelen te hebben genomen, maar ben je toch nog het haasje, omdat je nu net niet aan dat éne gaatje dacht. Hier een praktijkgeval, dat leert hoe een moment van onoplettendheid je anderhalf jaar later lelijk kan opbreken.

Begin oktober kreeg ik een factuur van CheapConnect. Daarbij bleek mijn volledige beltegoed van ca €13,- opgemaakt te zijn. In de logboeken blijkt dan, dat door onbekenden naar mobiele nummers in Engeland, Polen en Cuba is gebeld. Dat het om een klein bedrag gaat is een geluk bij een ongeluk, maar hoe was het schijnbaar onmogelijke toch een feit! Onderzoek …

Wachtwoord gestolen uit mijn netwerk? ... Uitgesloten!

Van alle systemen werd de beveiliging nog eens nauwkeurig nagelopen. Alle systemen zijn beveiligd met Windows Firewall. Eén systeem met NOD32 Antivirus, de drie andere met F-Secure, beveiligingssoftware die hun sporen wel hebben verdiend. Bovendien zit alles achter de firewall van de router.

Er wordt uitsluitend, door alle gebruikers, gewerkt onder een beperkt account. Niemand weet het wachtwoord van het beheersaccount, behalve ikzelf, en downloads worden alleen gedaan vanaf de site van te goeder naam en faam bekend staande leverancier. Als oorzaak uitgesloten!

Ingebroken bij CheapConnect? ... Uitgesloten!

Deze firma werkte niet echt mee aan het onderzoek. Ze leggen de oorzaak bij voorbaat bij de gebruiker en ook al zal dat vaak het geval zijn, heb ik een natuurlijke afkeer van conclusies, niet gebaseerd op onderzoek. Met enige moeite werd informatie gekregen over de herkomst van de onbevoegde telefoontjes, maar die is hier niet relevant.

Uiteindelijk is het namelijk onwaarschijnlijk dat het netwerk van CheapConnect is gehackt, want dan zou de wereld op zijn kop staan. Blijft de mogelijkheid dat daar alleen toegang werd gekregen tot mijn account. Ook dat is onwaarschijnlijk, want het wachtwoord bestaat daar uit 16 willekeurige tekens. Als oorzaak uitgesloten!

Een lek in de FRITZ!Box 7360, verstrekt door XS4ALL? ... Uitgesloten!

Begin 2014 stond hierover inderdaad de wereld op zijn kop. Als de router op afstand benaderbaar was via https-poort 443, konden criminelen daaruit alle accounts en wachtwoorden halen. Dat lek heeft nooit in mijn 7360 gezeten, want die is mij pas in mei 2015 door XS4ALL verstrekt, voorzien van toen al volledig veilige firmware.

De box is zowel in LAN als WAN beveiligd met een wachtwoord van 16 willekeurige tekens en bovendien is een andere poort dan 443 gebruikt voor MyFritz. Ook hier kan het niet gebeurd zijn. Als oorzaak uitgesloten!

Maar wat dan wel? De film terugdraaien!

Dan oppert iemand de mogelijkheid dat het wachtwoord al in februari 2014 kan zijn buitgemaakt. Toen gebruikte ik bij UPC een FRITZ!Box 7390 aan de kabel. Hier komt mijn, zoals velen het noemen, beroepsdeformatie goed van pas. Ik bewaar alles, want kwaliteitsbeheersing vereist dat je de film in geval van een calamiteit kunt terugdraaien. Het configuratiebestand van toen is bewaard. Het is even een klus, want die 7390 doet nu dienst als WLAN-accesspoint voor de 5 GHz-band. Maar toch sla ik even zijn huidige configuratie en die van de huidige 7360 op. Dan worden alle telefoonverbindingen in de huidige box gewist, en wordt de 7390 aan het netwerk gehangen als hing het weer aan de kabel. De configuratie van januari 2014 wordt ingeladen …

En dan verschijnt meteen de oorzaak van het probleem, want CheapConnect is de enige verbinding die netjes wordt geregistreerd. Alle andere VoIP verbindingen komen er niet in. Keihard bewijs dat de het huidige wachtwoord voor CheapConnect nog hetzelfde is als dat van januari 2014.

En daarmee valt alles op zijn plaats. Het verklaart waarom alleen deze VoIP verbinding werd gehackt, want de andere wachtwoorden zijn meteen na het bekend worden van het lek gewijzigd. Waarom het wachtwoord van CheapConnect niet werd gewijzigd? Dat is helaas niet meer te achterhalen, maar van belang is wel dat de oorzaak van het probleem kon worden achterhaald. Ik weet nu dat na vervanging van het wachtwoord, deze verbinding weer veilig is.