Misbruik

Spookgesprekken en misbruik telefonie

Spookgesprekken zijn gesprekken die binnen komen op uw toestel. U wordt bijvoorbeeld gebeld door het nummer 1000, maar als u opneemt hoort u niks. Dit gebeurt omdat het toestel een pakket ontvangt waarvan het toestel denkt dat het een binnenkomende lijn is. Dit komt vanaf een apparaat in het netwerk wat mogelijk gehacked is. Er wordt dan door hackers getracht misbruik te maken van uw telefonie om zo gesprekken door te sluizen, met als gevold hoge gesprekskosten voor u.

Hoe herken ik spookgesprekken:
U kunt spookgesprekken herkennen doordat u wordt gebeld door een onbekend nummer of naam.
Een aantal voorbeelden van deze nummers zijn: 2000, 2001 ,1000 ,1001,1002,1003,1004,1005,1006, 1050 en 101 of de namen: sipvicious, sipcli*, iWar.
Dit zijn geen extensie's in uw PBX of telefooncentrale, maar enkel lokaal op het toestel.

Mogelijke oorzaken:

1. De gebruikte router / firewall heeft functies Hardware NAT en/of SIP ALG actief.
2. Een oudere modem/router bijvoorbeeld KPN Experia Box v8 of ouder.
3. Er staat een port forwarding open in de firewall naar het toestel.
4. Er is een computer gehacked, besmet met virus of trojan.
5. Een verstoring in het netwerk waardoor er UDP pakketen blijven rond gaan in het netwerk. Bijvoorbeeld meer dan 3 switches, gebruik van een netwerk HUB, een oude router zonder VoIP ondersteuning.

Mogelijke oplossingen:

1. De functie Hardware NAT staat aan in de router/firewall, dit dient uitgezet te worden.
2. De functie SIP ALG staat aan in de router/firewall, dit dient uitgezet te worden.
3. Schakel uw WiFi tijdelijk uit en zie of de gesprekken nog steeds plaatsvinden.
   Zo ja, dat komt het misbruik vanaf een gehacked draadloos apparaat, bijvoorbeeld een smartphone.
4. Wijzig uw WiFi wachtwoord.
5. Schakel alle computers tijdelijk uit en zie of het intern bellen stopt.

   Wanneer het bellen stopt, dan is één van de computers gehacked.
6. Herstarten van het netwerkapparatuur.
7. Herstarten apparatuur, zoals computers toestellen en basisstation.
8. Portforwardings uitzetten.
9. De modem/router vervangen.
10. Als laatste kunt u ook het betreffende toestel, tijdelijk, als enige apparaat aansluiten op uw

    firewall.

Zie ook de overige items in de categorie misbruik.

Unieke FAQ ID: #1315
Auteur: Helpdesk
Laatst bijgewerkt:2018-08-15 01:33