AYI NEDJIMI Consultants

Équipements en fin de vie : le maillon faible que personne ne veut voir

Catégorie : Cybersécurité Générale Lecture : 7 min Publié le : 29/03/2026 Auteur : Ayi NEDJIMI

Les équipements en fin de vie sont le maillon faible oublié de la cybersécurité. Routeurs D-Link, smartphones Android sans patch : analyse et plan d'action concret.

Des routeurs D-Link exploités depuis quatre mois sans correctif possible. Des smartphones Qualcomm vulnérables que leurs constructeurs ne patcheront jamais. Des appliances VMware en production depuis six ans sans mise à jour. Ce n'est pas de la fiction : c'est l'état réel de milliers d'infrastructures en France en mars 2026. Et le problème ne fait que s'aggraver.

Le déni collectif autour des équipements EOL

Quand un éditeur annonce la fin de support d'un produit, la majorité des organisations… ne font rien. Le routeur fonctionne encore. Le serveur tourne. Le téléphone passe des appels. Pourquoi remplacer quelque chose qui « marche » ? Ce raisonnement est exactement celui sur lequel comptent les attaquants.

Les chiffres parlent d'eux-mêmes. En mars 2026, la faille CVE-2026-0625 sur les routeurs D-Link DSL en fin de vie est exploitée activement depuis novembre 2025 — plus de quatre mois. D-Link a confirmé qu'aucun patch ne sera publié. Pendant ce temps, ces routeurs compromis sont recyclés en botnets, en proxys pour du trafic malveillant, en points d'interception DNS. Et leurs propriétaires n'en savent rien.

Un problème systémique, pas anecdotique

Ce n'est pas un cas isolé. Le bulletin Android de mars 2026 corrige CVE-2026-21385, une faille Qualcomm touchant plus de 200 chipsets. Combien de ces appareils recevront effectivement le correctif ? Sur les smartphones de plus de trois ans : probablement aucun. La fragmentation Android transforme chaque fin de support constructeur en vulnérabilité permanente, comme nous l'avons documenté dans notre analyse de la forensique mobile.

Côté infrastructure, même constat. Les botnets IoT qui battent des records de DDoS ne s'appuient pas sur des zero-days sophistiqués. Ils exploitent des failles connues sur des équipements que plus personne ne maintient. Le ratio effort/impact pour l'attaquant est imbattable : un seul exploit, des millions de cibles, zéro risque de patch.

Pourquoi les organisations ne bougent pas

Trois raisons reviennent systématiquement sur le terrain :

Le budget. Remplacer un parc de routeurs ou de téléphones professionnels coûte cher. Mais c'est un calcul à courte vue : le coût d'un incident (forensique, remédiation, notification RGPD, perte de confiance) dépasse systématiquement celui du remplacement préventif. Les organisations qui ont subi des audits RGPD le savent bien.

La visibilité. Beaucoup d'organisations ne savent tout simplement pas quels équipements tournent sur leur réseau, encore moins leur statut de support. Sans inventaire à jour, impossible de prioriser les remplacements. C'est la base d'un audit de sécurité SI rigoureux.

L'inertie. « Ça a toujours été là, ça fonctionne. » Le biais du statu quo est le meilleur allié des attaquants. Tant qu'il n'y a pas d'incident visible, le risque reste abstrait pour la direction.

Ce qu'il faut faire concrètement

La gestion du cycle de vie des équipements n'est pas un luxe — c'est un fondamental de sécurité au même titre que le patch management logiciel. Voici les actions prioritaires :

- **Inventorier exhaustivement** tous les équipements réseau, IoT et terminaux mobiles du parc, avec leur date de fin de support. Des outils comme Lansweeper, GLPI ou même un simple scan Nmap régulier permettent de détecter les fantômes du réseau.
- **Définir une politique de remplacement** proactive : tout équipement à moins de 12 mois de sa fin de support doit avoir un successeur identifié et budgété.
- **Isoler en attendant** : les équipements EOL qui ne peuvent pas être remplacés immédiatement doivent être segmentés dans un VLAN dédié, avec un monitoring renforcé et un accès réseau minimal.
- **Intégrer le cycle de vie dans les achats** : avant de déployer un nouvel équipement, exigez du fournisseur un engagement écrit sur la durée de support sécurité. Cinq ans minimum, sans discussion.

Mon avis d'expert
Je le dis sans détour : la gestion des équipements en fin de vie est le trou béant le plus prévisible et le plus ignoré de la cybersécurité française. Pas par manque de compétences — par manque de volonté budgétaire et politique. Quand je fais un audit réseau en PME, je trouve systématiquement des équipements EOL exposés sur Internet. Systématiquement. Le jour où un régulateur imposera un inventaire certifié du matériel actif avec preuve de support, beaucoup de DSI vont avoir une très mauvaise surprise. En attendant, chaque routeur D-Link oublié dans un placard est une porte grande ouverte sur votre SI.

Conclusion

Les zero-days font les gros titres. Mais les vraies brèches, celles qui perdurent des mois en silence, exploitent des failles connues sur des équipements que personne ne surveille plus. La question n'est pas de savoir si vos équipements EOL seront exploités — c'est de savoir quand. Et pour beaucoup d'organisations, la réponse est : c'est déjà fait.

Ayi NEDJIMI Consultants — Expert cybersécurité offensive & intelligence artificielle

ayinedjimi-consultants.fr · ayi@ayinedjimi-consultants.fr