



Orange Cyberdefense compte 1200 collaborateurs et 250 millions d'euros de chiffre d'affaires.

# Le nouveau gardien de la cybergalaxie

**PAR MARY VAKARIDIS** Pour mieux contrer les attaques informatiques, le groupe télécom français Orange vient d'ouvrir à Paris un centre ultramoderne dédié à la cybersécurité. Il vise une place de leader européen.

« Il y a quelques années encore, lorsque vous étiez hacké, vous sentiez un peu idiot et coupable d'avoir négligé les règles de prudence. Mais aujourd'hui, plus personne n'est à l'abri. La piraterie informatique a maintenant atteint son âge industriel. Et les attaques coûtent de plus en plus cher aux victimes », décrypte Michel Van Den Berghe, directeur d'Orange Cyberdefense.

Cet automne à Paris, le groupe télécom français Orange inaugurerait à la Défense

son nouveau centre ultramoderne consacré à la sécurité informatique. Avec 1200 collaborateurs et un chiffre d'affaires de 250 millions d'euros, Orange Cyberdefense est devenu le leader français de ce secteur en deux ans. Gratte-ciel de 12 niveaux, le siège de prestige incarne cette réussite. A l'intérieur, du mobilier coloré comme chez Google, des employés jeunes et formés aux dernières techniques, des

**LES ATTAQUES COÛTENT DE PLUS EN PLUS CHER: 250 MILLIONS D'EUROS POUR SAINT-GOBAIN, MALMENÉ PAR LE MALWARE «PETYA»**

laboratoires dont les développements resteront dissimulés. La culture du secret fait partie de l'ADN des professionnels de la cybersécurité.

## «Empiler des sacs de sable»

Coté en bourse avec pour principal actionnaire l'Etat français (13,4%), le premier opérateur télécom français Orange emploie au total plus de 140 000 personnes. Fondateur d'Atheos, société de sécurité informatique acquise par Orange en 2014, Michel Van Den Berghe a rapidement pris la tête de l'ensemble de la division qui lui a racheté sa compagnie. «Le métier de la cybersécurité, c'est d'empiler des sacs de sable lorsque s'annonce une inondation. De la même manière, dès qu'une attaque est décelée, nous intervenons pour protéger les entreprises afin d'empêcher le virus d'atteindre les systèmes informatiques.»

L'argument massif en faveur de la nécessité d'une protection efficace, ce sont les coûts des dommages causés par les pirates. La facture de l'attaque WannaCry en mai dernier a atteint un total de 8 milliards de dollars pour l'ensemble de ses victimes. Chez Saint-Gobain, le malware (logiciel malveillant) Petya a oblitéré le chiffre d'affaires de 250 millions d'euros. Des dangers qui justifient pour une multinationale d'assurer sa sécurité pour une facture annuelle pouvant grimper jusqu'à 20 millions d'euros.

Chez Orange Cyberdefense, les ingénieurs ont constamment l'œil sur une multitude d'écrans muraux. Le nombre des attaques est vertigineux. Les dispositifs détectent 21 milliards d'événements suspects par jour. Une grande quantité des codes est identifiée et bloquée immédiatement. A l'issue du processus subsistent 85 incidents critiques par mois.

Une partie importante de la clientèle est constituée par les firmes stratégiques pour le fonctionnement du pays. Des entreprises et institutions que le gouvernement français a définies en tant qu'«opérateurs d'importance vitale» (OIV). Orange Cyberdefense a notamment pour mandat de déceler les failles sécuritaires en attaquant en permanence leurs systèmes informatiques.

## Chantage, phishing...

Du côté des pirates, les moyens sont en expansion constante. Les spécialistes distinguent quatre types d'attaques. Il y a d'abord les acteurs isolés aux motivations

variables. Ensuite, il existe des groupes de hackers comme Anonymous, soit des collectifs qui poursuivent des revendications communes.

La plus grande partie des effractions relève de malfaiteurs qui cherchent à s'enrichir en faisant par exemple du ransomware, c'est-à-dire du chantage après avoir installé un virus.

Enfin, les services de renseignement des Etats recourent aux mêmes armes. Un cas de figure apparu au grand jour lors de l'attaque des Etats-Unis en mai dernier attribuée à la Corée du Nord. Michel Van Den Berghe reprend: «Les administrateurs de réseau commencent même à être victimes de chantage physique et de menaces dirigées contre leurs enfants afin qu'ils livrent des codes d'accès et les mots de passe.»

Au registre des effractions, le phishing représente quelque 60% des activités globales d'Orange Cyberdefense. Ce fléau consiste à usurper l'identité de grandes compagnies à des buts d'escroquerie. «Nous sommes aussi très occupés par les retours d'attaques. Prenez le malware WannaCry. Son code a été publié comme celui de tous les virus. Toutes sortes de gens malintentionnés essaient ensuite de



**Michel Van Den Berghe: «La piraterie informatique a atteint son âge industriel.»**

répliquer l'opération», dévoile Michel Van Den Berghe.

Avec déjà 30% de ses revenus qui proviennent de l'étranger, Orange Cyberdefense vise une place de leader européen face à des concurrents comme Deutsche Telekom ou BT. En Suisse, la

firme compte notamment comme client le CICR (Comité international de la Croix-Rouge) dont les systèmes de communication doivent rester indétectables sur le terrain.

Si les grandes entreprises sont équipées d'outils antiransomware, en revanche, la protection des PME est encore à construire. Orange Cyberdefense développe pour 2018 une solution «cyber-filtre» qui nettoie les flux avant qu'ils arrivent chez le client. Une option à quelques euros par mois. Michel Van Den Berghe commente: «Un tel service revient à assurer que de l'eau potable sort du robinet.»

### **Pénurie de spécialistes**

Dans la cybersécurité, le plus gros défi, c'est le recrutement. En France, seuls quelque 1200 ingénieurs spécialisés par an arrivent sur le marché. Or 6000 postes, soit cinq fois plus, sont actuellement ouverts. Michel Van Den Berghe explique: «C'est pourquoi nous créons notre propre institut de formation. La pénurie débouche sur d'excellentes conditions de travail pour les professionnels. Un ingénieur en cybersécurité double son salaire en trois ans.» ■

# Bilan

PARTENAIRE MEDIA

**CREA DIGITAL DAY**  
GROUPE INSEC  
9<sup>e</sup> édition 2018

IMAGINÉ AVEC



# #CDD18

L'ÉVÈNEMENT DIGITAL #1 EN SUISSE ROMANDE

1 JOURNÉE / 20 ORATEURS / 1300 PARTICIPANTS

# 19 JANVIER 2018

Le CREA Digital Day revient pour évoquer les grands enjeux de 2018: digitalisation des entreprises, nouvelles technologies, industries émergentes et grands défis sociétaux.

📍 Théâtre du Léman  
Grand Hotel Kempinski

PROGRAMME & INSCRIPTIONS SUR  
[WWW.CREADIGITALDAY.COM](http://WWW.CREADIGITALDAY.COM)

ORACLE

Fédération des  
Entreprises  
Romandes  
Genève

digitalswitzerland

Medi@LAB

gfi

mediaprofil

PARTENAIRES MEDIA

Bilan

GOLDBACH  
MEDIA

tamedia

one

TRB