Quand la Cyber SÃ©curitÃ© devient un enjeu politique
Accessoire
PostÃ© par : JulieM
PubliÃ©e le : 29/11/2017 13:00:00

Pas une semaine ne se passe en 2017 sans quâ□□un Ã©vÃ©nement Â« Cyber Â» ne fasse la une des journaux. Que ce soit Ã travers des actes de ranÃ§onnage, de fuites dâ□□informations massives, de tentative dâ□□influence Ã©lectorales ou encore dâ□□actes de sabotages ou dâ□□espionnage, les Ã©vÃ©nements sâ□□enchaÃ®nent et sâ□□accÃ©lÃ¨rent depuis quelques mois. Dâ□□un sujet qui Ã©tait celui des spÃ©cialistes on bascule lentement mais surement dans le domaine commun.Â

En parallÃ¨le de ces Ã©vÃ©nements on observe aussi une forte poussÃ©e rÃ©glementaire et lÃ©gale sur les mÃªmes sujets avec lâ□□adoption de lois internes aux pays comme la loi de Programmation Militaire, ou de directives europÃ©ennes comme la GDPR ou la NIS. De lÃ Ã dire que la Cyber SÃ©curitÃ© devient un enjeu et pourquoi pas un jeu politique il nâ□□y a quâ□□un pas.



CommenÃ§ons par lâ□□enjeu. Les travaux effectuÃ©s par un groupe dâ□□experts menÃ© par par le CCDCOE (NATO Cooperative Cyber Defence Centre of Excellence) et publiÃ©s par lâ□□universitÃ© de Cambridge Ã travers le document Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations sont le meilleur exemple des enjeux associÃ©s Ã la cyber sÃ©curitÃ© au niveau mondial.

De la mÃªme maniÃ¨re lâ□□engagement fort des pays, notamment en Europe, Ã la mise en

place dâ□□organisation Ã©tatique en charge de lâ□□approche dÃ©fensive mais aussi offensive de la nation montre bien lâ□□importance vitale que prend aujourdâ□□hui la cyber sÃ©curitÃ© dans la vie du citoyen et dans la stabilitÃ© des nations.

La causalitÃ© ou la consÃ©quence de tout cela selon les cas est dâ□□entrevoir la disparition de la frontiÃ¨re entre monde rÃ©el et monde cyber. Nous avons pu observer en 2017 une symÃ©trie forte entre les Ã©vÃ©nements Â« rÃ©els Â» et les Ã©vÃ©nements Â« Cyber Â», Ã titre dâ□□exemple :

Â· ***Les activitÃ©s fortes de la CorÃ©e Du Nord*** en rÃ©ponse au boycott international par lâ□□utilisation dâ□□attaques malveillantes sur des plateformes dâ□□Ã©change de crypto-monnaies afin de rÃ©unir des fonds pour le parti au pouvoir (Lien sur BLOG associÃ©)

Â· ***Lâ□□utilisation massives et rÃ©pÃ©tÃ©es des actes de malveillances Cyber*** en Ukraine de la part dâ□□acteurs associÃ©s Ã la Russie (NotPetya â□□ BlackEnergy â□□ BadRabbit) comme outils de guerres.

Â· Les tentatives dâ□□influence de la part dâ□□APT28 (LIEN WITHEPAPER) et APT29 associÃ©s Ã lâ□□Ã©tat russes lors des Ã©lections EuropÃ©ennes ou AmÃ©ricaines qui ont Ã©tÃ© utilisÃ©es de maniÃ¨res massives et associÃ©es Ã des fuites dâ□□information volontaires (MACRON LEAK) ou Ã des fake news ayant lâ□□objectif de dÃ©crÃ©dibiliser un candidat ou un parti.

Â· Le cyber espionnage utilisÃ© par des groupes associÃ©s Ã lâ□□Iran pour rattraper un retard technologique dans les verticales de business les plus importantes pour lâ□□Ã©tat comme lâ□□hydrocarbure ou le transport aÃ©rien. (APT33)

On constate clairement quâ□□aujourdâ□□hui la cyber capacitÃ© devient outils de lâ□□arsenal des Ã©tats dans leurs capacitÃ©s Ã se protÃ©ger, Ã progresser ou pourquoi pas Ã attaquer. Et le citoyen me direz-vous dans tout cela, il peut malheureusement devenir une victime collatÃ©rale de ces Ã©vÃ©nements. Nous avons Ã ce jour peu ou pas de morts officiellement associÃ©s Ã un Ã©vÃ©nement Cyber mais cela peut et arrivera sÃ»rement un jour, lors dâ□□une utilisation destructrice de code malveillants comme nous lâ□□avons vu dans des cas tels que Shamoon 2.0 ou APT33.

Il reste un point sous-estimÃ© Ã mon sens dans les pays occidentaux : le pillage du patrimoine informationnel des entreprises. A mon sens il sâ□□agit dâ□□un enjeu de stabilitÃ© Ã©conomique et politique. Ce sujet malheureusement ne fait pas toujours lÃ une des mÃ©dias car lui est plus pernicieux, il nâ□□est pas tout de suite visible, nÃ©anmoins aujourdâ□□hui nous rÃ©pondons Ã de nombreux incidents Ã travers le monde mettant en exergue cette pratique de pillage. Un des groupes les plus actifs Ã ce sujet est APT10 dont sa spÃ©cialitÃ© est la rÃ©cupÃ©ration de propriÃ©tÃ©s intellectuelles en Europe.

A la lumiÃ¨re de ces Ã©lÃ©ments, 2 conclusions me viennent : la cyber est et sera de plus en plus prÃ©gnante dans la politique des Etats et chaque opÃ©ration de la vie rÃ©elle risque dâ□□avoir sa rÃ©sonnance cyber dans les prochaines annÃ©es. Et enfin que lâ□□attribution des actes va devenir un sujet de prÃ©occupation important, car pour se dÃ©fendre il faut comprendre et pour rÃ©pondre il faut savoir qui est derriÃ¨re une attaque.

Une menace dans le monde virtuel est un sujet complexe et plein de zones dâ□□ombre, dont on nâ□□a pas fini de parler.

David Grout Director Technical - PreSales, South EMEA de FireEye