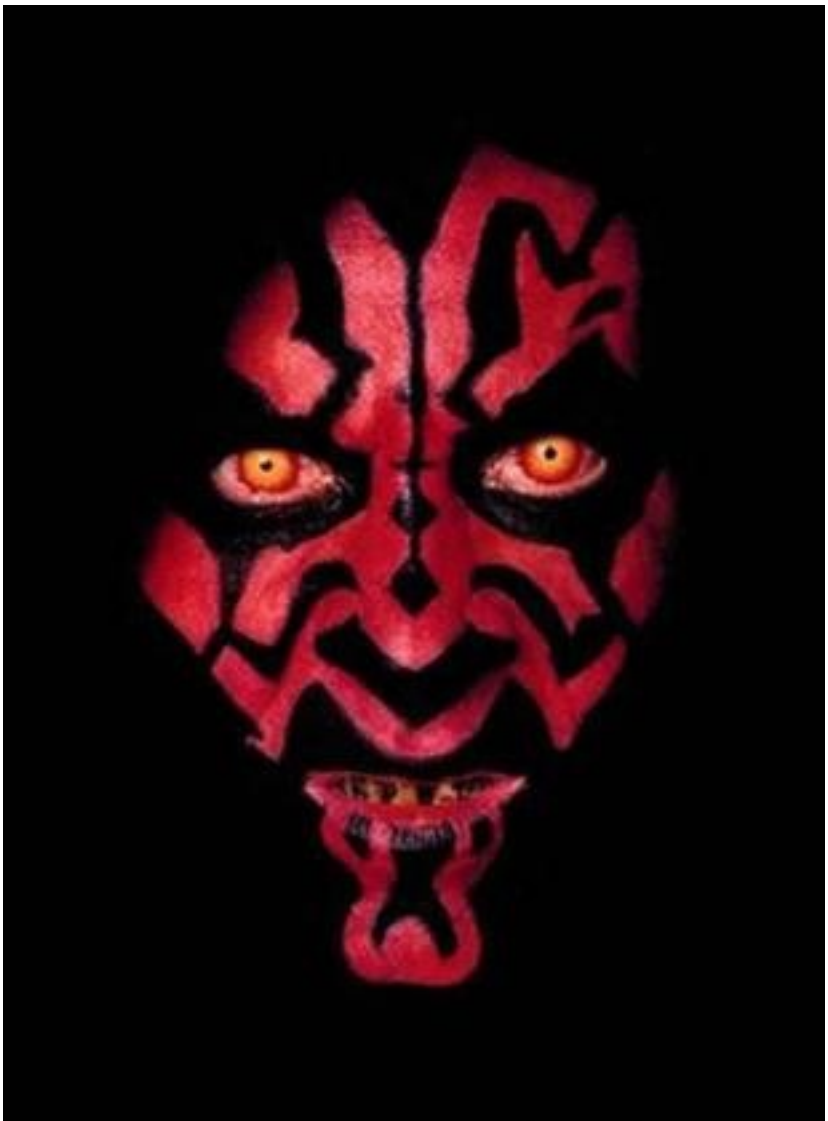
RGPD, PSD2, ransomware, IoT, cryptomonnaies : Danger en 2018
Internet
PostÃ© par : JPilo
PubliÃ©e le : 28/11/2017 13:30:00

Cette Ã©poque de lâ□□annÃ©e est toujours propice Ã une petite rÃ©flexion sur les douze mois Ã©coulÃ©s, et â□□ Ã©lÃ©ment peut-Ãªtre plus important encore â□□ sur ce que lâ□□avenir est censÃ© nous rÃ©server. Je me souviens avoir participÃ© il nâ□□y a pas si longtemps, quelques annÃ©es tout au plus, Ã un certain nombre dâ□□analyses prospectives Ã cinq ou dix ans.

Face au rythme des Ã©volutions technologiques, la plupart considÃ©reraient aujourdâ□□hui cet horizon de prÃ©vision bien trop Ã©loignÃ©. Sur cette mÃªme Ã©chelle temporelle, lâ□□annÃ©e paraÃ®t, a contrario, rÃ©duite Ã un bref instant. Quelques rÃ©flexions sur les phÃ©nomÃ¨nes qui risquent de se produire dans lâ□□annÃ©e qui vient, assorties de suggestions sur la maniÃ¨re de les gÃ©rer. Selon toute vraisemblance, leur incidence se fera sentir durant quelques annÃ©es.



Les cyberattaques nâ□□auront pas les mÃªmes rÃ©percussions. Ã□ la lumiÃ¨re de certaines attaques aux ranÃ§ongiciels lancÃ©es en 2017 qui ont impactÃ© des structures mÃ©dicale, il est manifeste que les cyberincidents ont Ã prÃ©sent des rÃ©percussions rÃ©elles et concrÃ¨tes sur les individus.

Avec lâ□□essor du digital twin ou Â« jumeau numÃ©rique Â» (autrement dit la crÃ©ation dâ□□un double digital pour chaque processus ou systÃ¨me en place), il faut sâ□□attendre Ã ce que ce phÃ©nomÃ¨ne sâ□□amplifie et sâ□□Ã©tende Ã de nombreux autres aspects de notre quotidien.

Dans quelle mesure la cybersÃ©curitÃ© sâ□□en trouvera-t-elle donc modifiÃ©e ?

Il est trÃ¨s probable que dâ□□autres dispositions rÃ©glementaires verront Ã nouveau le jour, continuant Ã durcir les critÃ¨res de sÃ©curitÃ© et Ã faire renaÃ®tre la confiance dans des cyber-systÃ¨mes qui ont un impact sur la collectivitÃ©.

La Directive NIS sur la sÃ©curitÃ© des rÃ©seaux et des systÃ¨mes dâ□□information, qui sera applicable en 2018, prÃ©voit une nouvelle catÃ©gorie de Â« fournisseurs de service numÃ©rique Â».

Au vu des rÃ©percussions tangibles considÃ©rables quâ□□ont les cyber-incidents sur la sociÃ©tÃ©, il faut sâ□□attendre Ã voir se multiplier les catÃ©gories du mÃªme acabit, par-delÃ les infrastructures nationales critiques dÃ©finies par le passÃ©, ou les opÃ©rateurs de services essentiels.

Dans ce contexte, le rÃ´le des responsables en charge de la sÃ©curitÃ©, comme le CSO (Chief Security Officer), doit Ã©voluer. Si des particuliers subissent un prÃ©judice imputable Ã une dÃ©faillance technologique, une enquÃªte publique sera probablement diligentÃ©e afin de dÃ©terminer sâ□□il y a eu nÃ©gligence et pourquoi, de dÃ©signer celui qui en porte la responsabilitÃ©, et de prendre les actions qui sâ□□imposent.

Par consÃ©quent si, tout rÃ©cemment encore, les CSO craignaient un Ã©ventuel licenciement en cas dâ□□incident, peut-Ãªtre est-ce la question de lâ□□engagement de leur responsabilitÃ© quâ□□ils devront redouter Ã lâ□□avenir. Cela aura-t-il pour effet dâ□□obliger les CSO Ã souscrire une assurance professionnelle, comme le font aujourdâ□□hui de nombreux professionnels de santÃ© ?

Est-il possible que, pour exercer en qualitÃ© de CSO, le professionnel en question doive satisfaire Ã certaines exigences et faire valoir la reconnaissance de ses compÃ©tences et son immatriculation Ã un rÃ©pertoire mÃ©tier, Ã lâ□□instar des professions rÃ©gies par le code de la santÃ© publique comme les mÃ©decins ?

Les principes directeurs appliquÃ©s depuis vingt ans nâ□□auront dÃ©finitivement plus cours. Nombre des principes directeurs rÃ©gissant la cybersÃ©curitÃ© nâ□□ont pratiquement pas Ã©voluÃ© en 20 ans.

Le plus souvent, les professionnels se sont efforcÃ©s de rÃ©soudre chaque problÃ¨me du mieux quâ□□ils pouvaient, en recourant aux solutions les plus efficaces Ã leur disposition Ã un instant t.

Cependant, eu Ã©gard aux Ã©volutions significatives des modÃ¨les de consommation informatique (des systÃ¨mes dynamiques et agiles, toujours plus consommables par nature, reposant sur un modÃ¨le de facturation Ã lâ□□abonnement), les entreprises cesseront dâ□□acheter et de dÃ©ployer des solutions de cybersÃ©curitÃ© cloisonnÃ©es distinctes exigeant des dÃ©penses dâ□□investissement et des compÃ©tences significatives, basÃ©es sur des cycles pluriannuels. Raison pour laquelle les paramÃ¨tres fondamentaux de consommation, dans le domaine de la cybersÃ©curitÃ©, Ã©volueront.

Pour fonctionner dans des environnements aussi dynamiques, les solutions de cybersÃ©curitÃ© doivent Ãªtre natives et automatisÃ©es, sâ□□exÃ©cuter et sâ□□adapter au mÃªme rythme.

Cela ne signifie pas, malgrÃ© tout, que le choix des fonctionnalitÃ©s technologiques et des

Ã©diteurs sera restreint â il suffit de jeter un Å il Ã la place de marchÃ© AWS pour sâen convaincre. Cela signifie, en revanche, que des fonctions dâallocation dynamique, de configuration et de transposition seront indispensables Ã une sÃ©curisation native.

NaguÃ¨re, la sÃ©curitÃ© a souvent Ã©tÃ© vouÃ©e Ã lâÃ©chec car les entreprises Ã©prouvaient Ã©normÃ©ment de difficultÃ©s Ã articuler leurs propres analyses et connaissances ; dans un univers informatique agile, il sera primordial de disposer dâun angle de visibilitÃ© intÃ©grÃ© et cohÃ©rent, couplÃ© Ã un contrÃ´le automatisÃ©.

Le caractÃ¨re Ã©phÃ©mÃ¨re de ressources informatiques toujours plus consommables crÃ©e un obstacle supplÃ©mentaire au sens oÃ¹, au moment oÃ¹ un incident est dÃ©couvert, lâenvironnement au sein duquel il a Ã©tÃ© engendrÃ© peut ne plus exister.

Vous devez donc Ãªtre en mesure de comprendre comment et pourquoi cet incident est survenu, Ã©tant donnÃ© que vous exercez vos activitÃ©s dans un univers de plus en plus rÃ©glementÃ©. Dâoù la nÃ©cessitÃ© de consigner et de prÃ©server les donnÃ©es historiques, et aussi de les mettre en corrÃ©lation pour pouvoir les exploiter.

Les cyber-assaillants se renforceront dans les ranÃ§ongiciels, les systÃ¨mes OT et les cryptomonnaies. Ces derniÃ¨res annÃ©es, les logiciels dâextorsion ont Ã©tÃ© utilisÃ©s Ã des fins lucratives. RanRan, lui, sâest servi du concept de ranÃ§ongiciel, non seulement dans ce but, mais aussi pour repÃ©rer des informations qui lui ont permis de faire chanter ses victimes.

En marge de la motivation financiÃ¨re, je suis convaincu que les ranÃ§ongiciels commenceront Ã©galement Ã mettre lâaccent sur lâanalyse des donnÃ©es ; dÃ¨s lors, les demandes de ranÃ§ons pourraient Ãªtre fonction de la valeur des donnÃ©es, et non plus gÃ©nÃ©riques, et il est Ã craindre que les attaques aux ranÃ§ongiciels, Ã des fins dâenrichissement ou pour dâautres motifs (chantage, par exemple), se multiplient.

Dans le cadre de lâattaque DDoS massive contre le gestionnaire de noms de domaine Dyn, les faiblesses de lâInternet des objets (IoT) et des appareils affÃ©rents ont Ã©tÃ© exploitÃ©es pour assaillir les systÃ¨mes informatiques traditionnels.

Alors que le volume de lâOT (technologies opÃ©rationnelles) affiche une progression soutenue, tant du cÃ´tÃ© des systÃ¨mes industriels que des drones livreurs de matÃ©riel mÃ©dical dans des pays comme lâAfrique, ces systÃ¨mes nâont pas encore fait les frais dâune attaque directe dont les rÃ©percussions restent Ã dÃ©finir.

NÃ©anmoins, compte tenu des sommes en jeu, des criminels voulant dÃ©rober ce matÃ©riel mÃ©dical chercheront certainement Ã infiltrer le rÃ©seau IoT ou le systÃ¨me OT pour dÃ©tourner les marchandises en question ; et câest bien lÃ la difficultÃ© quâil nous faudra surmonter.

Compte tenu de lâutilisation commerciale croissante des systÃ¨mes IoT et OT, le pirate a de plus en plus intÃ©rÃªt Ã les infiltrer pour en prendre le contrÃ´le.

Dernier point, avec lâessor des devises numÃ©riques, plus couramment dÃ©nommÃ©es cryptomonnaies, il faut sâattendre Ã ce que davantage de logiciels malveillants se polarisent sur le vol dâidentifiants et de coordonnÃ©es bancaires dans lâoptique de vider ces comptes de nouvelle gÃ©nÃ©ration.

La seconde directive europÃ©enne sur les services de paiement (PSD2) oblige les banques Ã Ã©largir lâaccÃ¨s de leurs systÃ¨mes de traitement des paiements Ã des tiers, et alors que les dÃ©bats se poursuivent autour de la blockchain et de ses grands livres comptables numÃ©riques, il semblerait que le secteur financier mette le cap sur les monnaies virtuelles.

La question est de savoir si les cyber-pirates sont prÃªts Ã profiter de cette phase transitoire â certains signes tendent dâores et dÃ©jÃ Ã montrer des vellÃ©itÃ©s en ce sens.

Le vol dâauthentifiants ciblera les fragilitÃ©s du cloud collaboratif au niveau des chaÃ®nes logistiques, tous acteurs confondus. Ã cause du phÃ©nomÃ¨ne Cloud ou dâune activitÃ© par essence dynamique, nous ne faisons, semble-t-il, que renforcer nos interconnexions avec nos partenaires, chaÃ®nes logistiques et clients.

Toute la difficultÃ©, ici, consiste Ã Åuvrer pour prÃ©server vos propres dispositifs de cybersÃ©curitÃ©, tout en cherchant Ã©galement Ã gÃ©rer les risques que vous font courir les autres (partenaires, chaÃ®ne logistique, etc.).

Dâaprï¿½s un atelier organisÃ© par IDC auquel jâai participÃ© dÃ©but 2017, le nombre de Clouds collaboratifs Ã vocation sectorielle sera multipliÃ© par cinq entre 2016 et 2018.

Face Ã des pirates toujours en quÃªte dâun point dâentrÃ©e leur permettant de sâinfiltrer dans lâentreprise, il paraÃ®t vraisemblable et logique que les espaces collaboratifs en mode Cloud constitueront leur prochaine porte dâentrÃ©e.

Dans ces conditions, les entreprises doivent commencer Ã rÃ©flÃ©chir aux types dâinformations quâil convient ou non dâexploiter dans ces espaces, aux mÃ©thodes Ã employer pour valider leur utilisation par les autres intervenants de maniï¿½re Ã pouvoir repÃ©rer les comportements anormaux, et â surtout â Ã la maniï¿½re dâisoler ces points de connexion des systï¿½mes mÃ©tier internes stratÃ©giques, en recourant Ã des mÃ©thodologies spÃ©cifiques telles que le modï¿½le ZÃ©ro confiance.

Pleins feux sur la recherche des responsabilitÃ©s et lâobligation de rendre des comptes. Depuis le modï¿½le partagÃ© de sÃ©curitÃ© en mode Cloud (la sÃ©curisation du Cloud incombant au prestataire, et celle de vos donnÃ©es vous appartenant) aux collaborations Cloud mutualisÃ©es, en passant par la demande de modï¿½les commerciaux plus ouverts dont la directive PSD2 se fait lâÃ©cho en entendant donner aux nouvelles offres Fintech les moyens de mieux rivaliser sur le marchÃ© des services de paiement, la complexitÃ© est le dÃ©nominateur commun.

Le nombre dâacteurs et de processus ne cessant dâaugmenter, ce qui accroÃ®t la marge dâerreur, il importe de mieux cerner les responsabilitÃ©s de chacun et de dÃ©terminer Ã qui incombe lâobligation de rendre des comptes, en jouissant dâune visibilitÃ© accrue.

En consÃ©quence, les entreprises Ã©plucheront trï¿½s certainement les clauses contractuelles et les dispositions rÃ©glementaires afin dâobtenir des rÃ©ponses claires sur ces points. De mÃªme, elles mettront un point dâhonneur Ã conserver des traces comptables et fichiers journaux circonstanciÃ©s, dÃ©taillant chaque transaction de maniï¿½re Ã pouvoir vÃ©rifier la date, la localisation et la cause des incidents.

De nouvelles rÃ©glementations europÃ©ennes notables vont faire leur apparition. Comme cela a dÃ©jÃ Ã©tÃ© Ã©voquÃ© dans dâautres prÃ©visions, un certain nombre de nouvelles rÃ©glementations entreront en vigueur en 2018. Concrï¿½tement, entre janvier et mai, le Rï¿½glement gÃ©nÃ©ral sur la protection des donnÃ©es (RGPD), la Directive NIS sur la sÃ©curitÃ© des rÃ©seaux et des systï¿½mes dâinformation, et la Directive sur les services de paiement (PSD2) deviendront applicables.

Comme pour toute lÃ©gislation nouvelle, il faudra du temps aux entreprises pour mesurer lâincidence de ces rÃ©glementations sur leur activitÃ©. Celles-ci prÃ©voient des sanctions potentiellement lourdes en cas dâinfraction. Autant dire que lâannÃ©e 2018 sera faste pour des entreprises qui seront confrontÃ©es Ã leurs implications concrï¿½tes, sâagissant de lâapplication des mesures de cybersÃ©curitÃ© et de la gestion de leurs obligations au quotidien.

Pour toutes ces raisons, je ne saurais trop vous encourager Ã vous intÃ©resser aux implications juridiques pour votre entreprise, au regard du droit comme de la pratique. Assurez-vous de disposer de lâ□□appui de votre direction et entamez, ou poursuivez, votre travail de mise en conformitÃ©. De plus amples informations sur le RGPD sont disponibles sur notre microsite.

La leÃ§on Ã tirer ? Prenez, pour 2018, la rÃ©solution de rendre la cybersÃ©curitÃ© plus agile. Dans un monde oÃ¹ le numÃ©rique se gÃ©nÃ©ralise, le rythme des transformations nâ□□est certainement pas linÃ©aire : il est exponentiel. Je vous recommande dâ□□ailleurs un excellent ouvrage, Ã lire entre les fÃªtes de fin dâ□□annÃ©e : Exponential Organisations signÃ© Salim Ismail.

La plupart des professionnels de la sÃ©curitÃ© ont aujourdâ□□hui renoncÃ© aux analyses prospectives, le rythme auquel sâ□□opÃ¨re le changement rendant impossible toute prÃ©vision plusieurs annÃ©es Ã lâ□□avance ; comme pour la tÃ©lÃ©phonie mobile, les cycles de vie informatique se rÃ©duisent comme peau de chagrin, et ne se chiffrent plus en annÃ©es, mais en mois. Dans le mÃªme temps, les interconnexions et, par association, les dÃ©pendances se multiplient, occasionnant un renforcement des contraintes rÃ©glementaires.

DÃ¨s lors, la cybersÃ©curitÃ© doit impÃ©rativement gagner en agilitÃ© pour ne pas se faire distancer. Ã□ lâ□□instar des ressources DevOps, nous devons Ãªtre prÃªts Ã Ã©voluer par paliers, Ã une frÃ©quence quotidienne ou hebdomadaire. Mais comment y parvenir ?

Il y a quelques annÃ©es, en enquÃªtant auprÃ¨s de certains de mes homologues, il mâ□□est apparu que ceux-ci consacraient la majoritÃ© de leur temps et de leurs ressources Ã pÃ©renniser lâ□□infrastructure de cybersÃ©curitÃ© quâ□□ils avaient Ã©rigÃ©e, et trÃ¨s peu Ã la faire Ã©voluer.

Si nous devons passer Ã lâ□□Ã©chelle supÃ©rieure, il faut impÃ©rativement revoir lâ□□utilisation de notre temps et de nos ressources, câ□□est-Ã -dire consacrer une petite part de celle-ci Ã consolider lâ□□infrastructure en place, et rÃ©server lâ□□essentiel au dÃ©veloppement de lâ□□agilitÃ© exponentielle quâ□□attendent nos entreprises.

Sur la liste de vos bonnes rÃ©solutions pour le Nouvel an, pensez donc Ã faire suivre Ã votre infrastructure une Â« cure dÃ©tox Â» qui vous permettra dâ□□aller de lâ□□avant et dâ□□envisager lâ□□avenir plus sereinement.