IBM : Lutte contre les cyber menaces grÃ¢ce Ã un systÃ¨me global de protection
SÃ©curitÃ©
PostÃ© par : JPilo
PubliÃ©e le : 6/5/2014 11:00:00

IBM aide ses clients Ã dÃ©tecter, prÃ©venir et rÃ©pondre au mieux aux attaques dans un contexte dâ□□augmentation du coÃ»t liÃ© aux violations des donnÃ©es et des menaces persistantes avancÃ©es (Advanced Persistant Threats)
IBMÂ prÃ©sente un nouveau systÃ¨me de sÃ©curitÃ© incluant des logiciels et des services qui aident les entreprises Ã protÃ©ger leurs donnÃ©es critiques dans un contexte dâ□□augmentation des menaces persistantes avancÃ©es , des vulnÃ©rabilitÃ©s informatiques Â« zÃ©ro jour Â», des infractions et des coÃ»ts qui en rÃ©sultent. GrÃ¢ce Ã une analyse gÃ©nÃ©ralisÃ©e des comportements et une expertise de recherche approfondie, IBM peut aider les entreprises Ã arrÃªter les personnes qui exploitent ces vulnÃ©rabilitÃ©s.

Selon deux enquÃªtes commandÃ©es par IBM auprÃ¨s de lâ□□institut Ponemon , le coÃ»t moyen de la violation des donnÃ©es a augmentÃ© de 15%, pour atteindre une moyenne de 3,5 millions de dollars. Les Ã©tudes indiquent Ã©galement que les attaques ciblÃ©es sont considÃ©rÃ©es comme la plus grande menace par la majoritÃ© des entreprises. Leur coÃ»t est estimÃ© Ã $ 9,4 millions de perte en valeur intrinsÃ¨que pour la marque.

L'arrivÃ©e dâ□□IBM Threat Protection System et de Critical Data Protection Program reprÃ©sente deux annÃ©es d'investissements significatifs en matiÃ¨re de croissance organique et d'acquisitions d'entreprises telles que Q1 Labs, Trusteer, Guardium, Ounce Labs, Watchfire et Fiberlink/MaaS360.

Depuis la mise en place, fin 2011, dâ□□un business dÃ©diÃ© Ã la cyber-sÃ©curitÃ©, IBM sâ□□est dÃ©veloppÃ© pour devenir l'un des plus grands acteurs en matiÃ¨re de sÃ©curitÃ© pour l'entreprise et est fort de six trimestres consÃ©cutifs de croissance Ã deux chiffres dans ce domaine. Selon l'indicateur de rÃ©fÃ©rence de la mesure du revenu logiciel par Ã©diteur, IBM a distancÃ© de faÃ§on significative le marchÃ© du logiciel de sÃ©curitÃ©, et est passÃ© en 2013 de la 4 Ã la 3Ã¨me place des plus grands fournisseurs de sÃ©curitÃ©.

IBM Threat Protection System peut prÃ©venir les attaques - avant quâ□□elles nâ□□arrivent

Le nouveau systÃ¨me de protection Threat Protection System contre les menaces d'IBM exploite les

renseignements liÃ©s Ã la sÃ©curitÃ© afin dâ□□aller au-delÃ des dÃ©fenses et des pare-feu traditionnels, ceci pour perturber les attaques Ã travers l'ensemble de la chaÃ®ne d'attaque, de lâ□□infiltration Ã lâ□□exfiltration.

IBM Threat Protection System comprend une architecture de logiciels d'analyse et dâ□□enquÃªte (forensics) de bout en bout. Ces derniers aident les organismes Ã prÃ©venir en continu, dÃ©tecter et rÃ©pondre aux cyber attaques complexes, en cours, et, dans certains cas, Ã Ã©liminer la menace avant que le dommage ne se soit produit.

- Pour la prÃ©vention, IBM annonce une nouvelle solution, Trusteer Apex, destinÃ©e Ã bloquer les logiciels malveillants, d'importantes amÃ©liorations pour IBM Network Protection afin de mettre en quarantaine les attaques, ainsi que de nouvelles intÃ©grations avec les partenaires clÃ©s bÃ©nÃ©ficiant des capacitÃ©s du rÃ©seau des Â« bacs Ã sable Â» testant les logiciels/programmes douteux (sandbox).

- Pour la dÃ©tection, IBM a amÃ©liorÃ© sa plateforme QRadar Security Intelligence en la dotant de nouvelles fonctionnalitÃ©s - permettant aux entreprises de dÃ©tecter les attaques Ã grande Ã©chelle et de les bloquer en un clic.

- Pour rÃ©pondre aux attaques, IBM a introduit IBM sÃ©curitÃ© QRadar Incident Forensics. IBM continue Ã©galement Ã Ã©tendre ses services d'intervention d'urgence Ã l'Ã©chelle mondiale.

Les clients qui ont testÃ© IBM Threat Protection System ont vu des rÃ©sultats rapides. Par exemple, un fournisseur de soins de santÃ© avec des milliers de terminaux a immÃ©diatement dÃ©tectÃ© la prÃ©sence de dizaines de cas de logiciels malveillants, malgrÃ© lâ□□utilisation habituelle de nombreux outils de sÃ©curitÃ© traditionnels. Ce code malveillant peut Ãªtre utilisÃ© pour contrÃ´ler Ã distance les terminaux ou exfiltrer des donnÃ©es, mais il a Ã©tÃ© immÃ©diatement dÃ©sactivÃ©. De mÃªme, une grande banque europÃ©enne a rÃ©cemment essayÃ© ce systÃ¨me et a Ã©tÃ© en mesure de dÃ©sactiver les logiciels malveillants dÃ©tectÃ©s dans l'entreprise.

Le systÃ¨me de protection contre les menaces IBM dÃ©pend de 11 centres d'opÃ©rations de sÃ©curitÃ© (SOC) qui peuvent surveiller le systÃ¨me une fois ce dernier dÃ©ployÃ© chez les clients.

Â« *Les menaces persistantes avancÃ©es ont fondamentalement modifiÃ© la maniÃ¨re dont les entreprises doivent aborder la question de la sÃ©curitÃ© des donnÃ©es.* Â» DÃ©clare Brendan Hanigan, Directeur GÃ©nÃ©ral de IBM Security Systems.

Â« *Aujourdâ□□hui, se dÃ©fendre contre les cyber attaques nÃ©cessite plus d'une approche basÃ©e sur la signature ou le pÃ©rimÃ¨tre. Des capacitÃ©s dâ□□analyse approfondies et les forensics sont indispensables et doivent inclure la prÃ©vention au niveau des terminaux (les terminaux fixes, mobiles utilisÃ©s par les employÃ©s, les partenaires et mÃªmes les clients), la protection du pÃ©rimÃ¨tre et la capacitÃ© Ã se prÃ©munir contre les attaques avant qu'elles ne causent des dÃ©gÃ¢ts* Â».

IBM Security Services protÃ¨ge les Â« Joyaux de la Couronne Â» d'une entreprise et la marque

Le nouveau Critical Data Protection Program permet de protÃ©ger les donnÃ©es critiques d'une organisation, ou notamment Â« Joyaux de la Couronne Â». La richesse d'une entreprise est souvent gÃ©nÃ©rÃ©e par moins de 2% de ses donnÃ©es, ce qui a un impact majeur sur la rÃ©putation de la marque, sa valeur de marchÃ© et sa croissance.

Â« *Les inquiÃ©tudes sur la capacitÃ© Ã protÃ©ger les donnÃ©es critiques contre les cyber*

attaques sont un prÃ©occupation du Board Â», a dÃ©clarÃ© Kris Lovejoy, Directeur GÃ©nÃ©ral de IBM Security Systems. Â« *Les cyber-attaques et la perte de donnÃ©es jouent un rÃ´le sur la rÃ©putation de marque, peuvent rÃ©duire sa valeur en actions et confronter une entreprise Ã des litiges. Les nouveaux logiciels et services d'IBM sont conÃ§us pour fournir Ã ces responsables une solution unique qui leur permet de focaliser leur attention sur les besoins de leurs clients et les revenus de l'entreprise au jour le jour* Â».

Les organisations font de plus en plus appel Ã IBM pour les aider Ã construire une approche vÃ©ritablement globale et intelligente pour identifier rapidement et bloquer les menaces avancÃ©es avant quâ□□elles ne fassent des dÃ©gÃ¢ts. RÃ©cemment, IBM a commencÃ© Ã fournir des services de soutien hotline par des experts et un dÃ©chiffrage des vulnÃ©rabilitÃ©s Ã ses assurÃ©s CyberEdge d'AIG.

Â« *Nous nous rÃ©jouissons quâ□□IBM continue de miser sur sa capacitÃ© unique Ã combiner logiciel leader sur le marchÃ©, services, capacitÃ©s de recherche et partenariats avec l'industrie pour contrer l'augmentation des attaques sophistiquÃ©es* Â», a dÃ©clarÃ© Tracie Grella , Head of Professional Liability, Global Financial Ã AIG.

Les nouveaux services de conseil en sÃ©curitÃ© sont basÃ©s sur le Data Centric Security Model d'IBM. Ce qui permet de protÃ©ger les informations critiques ou business les plus sensibles pour une entreprise en utilisant les fonctionnalitÃ©s de Guardium, StoredIQ et IBM Research.

Ces donnÃ©es critiques sont Ã forte valeur ajoutÃ©e comme les plans d'acquisition et de cession, les dÃ©libÃ©rations du Conseil exÃ©cutif et de la propriÃ©tÃ© intellectuelle. Ces donnÃ©es critiques correspondent Ã 70 % de la valeur d'une sociÃ©tÃ© cotÃ©e en bourse et sâ□□avÃ¨rent extrÃªmement prÃ©cieuses pour les forces hostiles â□□ que sont les initiÃ©s de la sociÃ©tÃ© ou les attaquants sophistiquÃ©s.

MalgrÃ© l'importance et la valeur des donnÃ©es critiques, de nombreuses organisations ne sont pas conscientes de ce quâ□□elles reprÃ©sentent, dâ□□oÃ¹ elles se trouvent, de qui y a accÃ¨s, ou de comment elles sont protÃ©gÃ©es, ce qui les rend plus difficiles Ã surveiller et Ã protÃ©ger.

En fait, la dÃ©couverte de la perte de donnÃ©es peut prendre des jours ou plus dans plus de 95 % des cas, et il faut des semaines ou plus pour les contrÃ´ler dans plus de 90% des cas, un dÃ©calage qui peut avoir un impact catastrophique pour une entreprise.

Le nouveau programme de protection des donnÃ©es critiques d'IBM propose une approche itÃ©rative multi-Ã©tapes : DÃ©finir, DÃ©couvrir, Comparer, SÃ©curiser et Surveiller. Ceci pour un cycle de vie complet en matiÃ¨re de sÃ©curitÃ© des donnÃ©es pour protÃ©ger la rentabilitÃ©, la position concurrentielle et la rÃ©putation.