HEXATRUST

CYBERSECURITY & DIGITAL TRUST

SECURISATION DE LA MESSAGERIE

Outils essentiels à la collaboration, les messageries sont devenues le principal vecteur d'attaque pour les cybercriminels

Selon le FBI, les entreprises dans le monde ont perdu plus d'1 milliard de dollars US entre octobre 2013 et juin 2015 du fait de fraudes à la messagerie professionnelle. La messagerie constitue, aujourd'hui, l'une des fonctions les plus visibles, les plus interconnectées et les plus déployées de l'IT, par conséquent, l'une des plus sensibles. Elle est le pilier de la collaboration en entreprise : le facteur humain y est donc critique. Les attaques sont, elles, très diversifiées. Elles peuvent être classiques, instantanées ou de longue haleine, et viser tout type de flux (mobile, voix, data, etc.) comme tous les moyens existants d'interaction et de stockage.

VISION PAC

A CXP GROUP COMPANY

Selon une enquête du FBI, les victimes de d'e-mails malveillants ont augmenté de 270% en 2014. Les messageries représentent l'un des actifs les plus importants du système d'information. Elles constituent un moyen primordial de communication et de collaboration, dont l'arrêt risque de paralyser l'activité d'une entreprise ou d'une administration. En outre, elles véhiculent et hébergent des **données** parfois très **sensibles**. Prévenir d'éventuelles attaques sur les messageries et s'en protéger est donc capital.

La diversité des systèmes de messageries, leurs liens avec le système d'information (portails, cloud, collaboration, etc.), avec les médias sociaux et avec les autres systèmes de sécurité (gestion des identités et des accès, gouvernance, confidentialité, sécurisation des flux mobiles, etc.) rend leur sécurisation particulièrement **complexe**.

La protection des messageries repose sur la sécurisation des boîtes de messageries, des flux de messageries, des divers terminaux, des systèmes, qu'ils soient hébergés dans l'entreprise ou dans le **cloud**. Leur sécurisation dépend également des interventions humaines, premier vecteur de vulnérabilité.

Critiques et sensibles, les messageries sont fortement impactées par les régulations, qu'elles soient nationales, continentales, internationales ou sectorielles.

Sécuriser de manière **holistique** est d'autant plus difficile que les menaces qui pèsent sur les messageries sont nombreuses. Les principales **menaces** sont :

- L'usurpation de mots de passe, des listes de diffusion et des modes d'accès à la messagerie via les applications ;
- L'utilisation de comptes à privilèges ;
- L'interception de données dans le flux ;
- Le vol de données
- Le phishing ;
- La protection de la réputation SMTP (bot qui envoie du spam depuis la messagerie) ;
- Les malwares ;
- Les spams.

L'avènement du Digital limite aujourd'hui l'efficacité des outils de sécurisation classiques, créant un **marché dual**. D'une part, la sécurisation de la messagerie est l'un des volets les plus matures de la Cyber Sécurité avec des fonctions telles que l'anti-virus, l'anti-spam, les gateways, etc. D'autre part, la persistance des attaques, et surtout leur succès, a stimulé le développement de **nouvelles approches** et solutions.

Ces nouvelles approches reposent sur une vision globale et sur une analyse comportementale et contextuelle : c'est la seule manière de pouvoir maîtriser un telle complexité et l'impact des actions humaines.

RÉPONSE D'HEXATRUST

HEXATRUST
CYBERSECURITY & DIGITAL TRUST

Les membres d'**HEXATRUST** proposent une réponse globale basée sur l'analyse **comportementale** et **contextuelle** des vulnérabilités et des menaces qui affectent les systèmes de messageries.

Les solutions proposées par les membres d'**HEXATRUST** protègent les entreprises de l'**usurpation d'identités**, de l'**interception** et **duplication de flux** ainsi que des **contenus malveillants** dans les flux entrants et sortants. Elles gèrent les comptes à privilèges, l'utilisation des listes de diffusion et l'utilisation abusive des boîtes de messagerie. Les solutions d'**HEXATRUST** analysent de manière exhaustive les flux de mails entrants et sortants afin de détecter en **temps réel** et **rétrospectivement** les malware, phishing, spam et mails commerciaux, le vol de données et les attaques sur les terminaux clients.

POSITIONNEMENT ET AVANTAGE D'HEXATRUST

Les membres d'**HEXATRUST** se positionnent comme fournisseurs de **solutions de haut niveau** pour sécuriser chacun des maillons de la chaîne de confiance des systèmes de messageries.

Au-delà de cette couverture, les solutions proposées par les membres d'**HEXATRUST** offrent, sur l'ensemble des fonctions couvertes, des capacités de détection permettant à l'utilisateur d'agir en **amont**, avant que l'attaque soit effective. Primordiales, la **détection** et la **prévention** constituent les segments affichant la plus forte croissance dans les investissements en Cyber Sécurité, selon la dernière enquête de PAC sur la gestion des incidents en Europe en 2015.

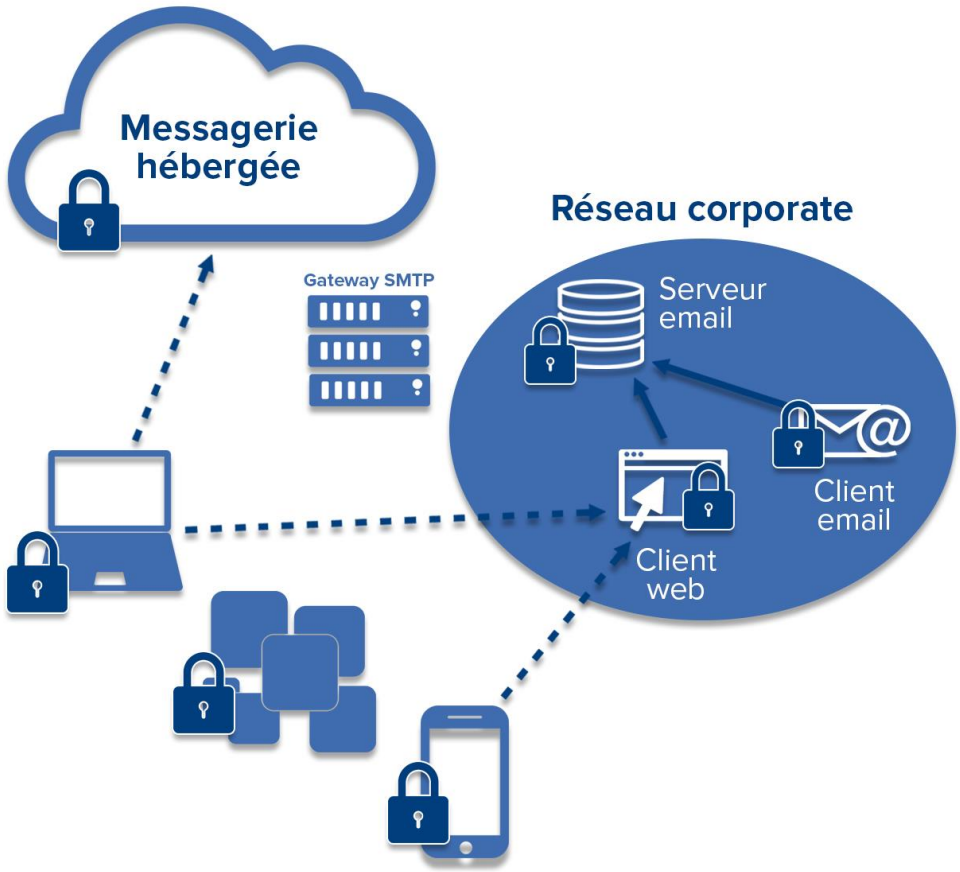
Dans l'offre d'**HEXATRUST**, ces capacités de détection sont renforcées par des **fonctions exploratoires avancées**, devenues essentielles du fait de la complexité et de la diversité des systèmes : on ne peut pas protéger un actif dont on ne connaît pas l'existence.

Un autre point critique dans la sécurisation des messageries est l'effet des interventions et interactions humaines. Alors que la plupart des concurrents d'**HEXATRUST** proposent des technologies basées sur une signature, le principal avantage des solutions d'**HEXATRUST** réside dans l'analyse **comportementale** et **contextuelle** qu'elles proposent. En permettant de comprendre l'impact des actions humaines sur tel ou tel système de messagerie, cette fonction différenciatrice est la seule capable de juguler la complexité inhérente aux systèmes digitaux.

Enfin, l'origine européenne d'**HEXATRUST** est un gage de **proximité**, mais aussi de **conformité** à certaines règlementations nationales très pointues.

Malgré l'ensemble de ces atouts, n'oublions pas l'essentiel : la **sensibilisation** des utilisateurs aux **risques**.

SÉCURISATION DE LA MESSAGERIE



L'Association HEXATRUST : HEXATRUST est née de la volonté commune de PME et ETI françaises, acteurs complémentaires experts de la sécurité des systèmes d'information, de la cyber sécurité et de la confiance numérique.

BRAINWAVE

38-42 rue Gallieni
92600 Asnières-sur-Seine – France
Tél : +33 1 84 19 04 10
jean-yves.pronier@brainwave.fr
www.brainwave.fr

Brainwave est un éditeur de logiciel focalisé sur l'Identity Analytics and intelligence. Notre mission est d'aider les entreprises à lutter contre la fraude, la fuite de données et les cyber risques, avec des solutions GRC analytiques novatrices. Brainwave renforce la sécurité informatique et la conformité par une analyse préventive des risques auxquels l'entreprise est exposée, que les applications et les données soient en interne ou dans le cloud.

denyall
NEXT GENERATION APPLICATION SECURITY

6 avenue de la Cristallerie
92310 Sèvres – France
Tél : +33 1 46 20 96 00
sdesaintalbin@denyall.com
www.denyall.com

DenyAll est un expert en sécurité applicative. DenyAll Web Application Firewall protège les accès web aux systèmes de messagerie d'entreprise et applications collaboratives, telles que Sharepoint et iNotes, contre les injections, cross-site scripting et autres attaques visant les couches applicatives. Il fournit un point de contrôle et d'authentification centralisé aux messageries cloud (comme gmail), afin de réduire les risques de fuite de données et d'usurpation d'identités. DenyAll Vulnerability Manager détecte les vulnérabilités des accès webmail et aide à les remédier, afin de réduire la surface d'attaque.

IDECSI

19-21 allée du parc de Garlande
92220 Bagneux – France
Tél : +33 9 53 72 44 91
contact@idecsi.com
www.idecsi.com

Idecsi protège totalement et sans aucune contrainte les mails des Dirigeants. Grâce à une solution de monitoring intelligent, les comptes mails bénéficient d'une protection permanente qui détecte immédiatement tout accès ou paramétrage malveillant. Une solution d'audit flash permet également de vérifier l'intégrité de n'importe quel compte mail : d'un clic, vous obtenez un diagnostic très précis.

inwebo
SECURITY BEYOND PASSWORDS

3 rue Montyon
75009 Paris – France
Tél : +33 1 46 94 68 38
sales@inwebo.com
www.inwebo.fr

InWebo propose un service d'authentification forte pour sécuriser l'accès à vos messageries. L'utilisation de la technologie de notification rend l'authentification extrêmement simple et intuitive, adoptée immédiatement par les utilisateurs. InWebo permet des déploiements aisés, massifs et sans délais de ses tokens hautement sécurisés et certifiés. Des connecteurs prêts à l'emploi sont notamment disponibles pour Office 365 ou Google for Work.

ITrust
IT SECURITY SERVICES

Bâtiment Actys/1
55 l'Occitane
31670 Labège – France
Tél : +33 5 67 34 67 80
mgodefroy@itrust.fr
www.itrust.fr

ITrust propose deux solutions afin de protéger la messagerie d'entreprise. 1. IKare, scanner de vulnérabilité, en tant qu'outil de prévention permet de déceler les failles de sécurité présentes au sein de l'application ou du/des serveur/s de messagerie. 2. Reveelium, analyse comportementale, en tant qu'outil de détection à partir des logs mails, permet d'identifier les comportements malveillants au sein de la messagerie et permet ainsi le blocage du phishing, de l'usurpation de comptes de messagerie, d'espionnage, d'extraction de données anormales.

NEOWAVE

Pôle d'activité Y. Morandat
1480 avenue d'Arménie
13120 Gardanne – France
Tél : +33 4 42 50 70 05
bruno.bernard@neowave.fr
www.neowave.fr

NEOWAVE propose sa solution Keydo FIDO U2F pour se protéger contre le phishing. Neowave est une société experte dans les domaines de l'authentification forte et des transactions sécurisées. Les produits de Neowave combinent le haut niveau de sécurité offert par la carte à puce avec des technologies de stockage et de connectivités : USB, technologies sans contact RFID/NFC, Bluetooth Low Energy (BLE).

PRIM'X
TECHNOLOGIES

117 avenue Victor Hugo
92100 Boulogne-Billancourt – France
Tél : +33 1 77 72 64 80
nicolas.bachelier@primx.fr
www.primx.eu

Prim'X Technologies développe des solutions de chiffrement pour lutter efficacement contre les accès non autorisés aux informations sensibles locales ou distantes, stockées ou échangées. La société propose ZedMail, plugin MsOutlook, pour le chiffrement de la messagerie de bout en bout et Zed, conteneurs multiplateformes pour le chiffrement des pièces jointes échangées et archivées. Zed est certifié EAL3+ et qualifié Standard par l'ANSSI, NATO Restricted et EU Restricted.

THEGREENBOW

28 rue de Caumartin
75009 Paris – France
Tél : +33 1 43 12 39 37
sales@thegreenbow.com
www.thegreenbow.fr

TheGreenBow est un éditeur français de logiciels de sécurité, spécialisé dans le chiffrement de données et la protection des communications. TheGreenBow est éditeur de la solution de chiffrement de mail Cryptomailer. CryptoMailer est la seule solution à proposer du chiffrement d'email de bout en bout, sur ordinateur, tablette ou smartphone, utilisable avec toute messagerie logicielle ou webmail.

VADE-RETRO
NEXT-GEN EMAIL FILTERING

3 avenue Antoine Pinay
Parc d'activité des 4 Vents
59510 Hem – France
Tél : +33 3 28 32 88 88
gregoire.lepoutre@vade-retro.com
www.vade-retro.com

Vade Retro protège 235 millions de mailbox dans 76 pays sur les marchés des FAI/Hébergeurs, OEM, et Entreprises. Les USP de Vade Retro sont Advanced Antiphishing Program permettant d'explorer les liens au moment du click de l'utilisateur, la lutte contre les malware polymorphe au niveau du content filtering, ainsi que la gestion des mails non-prioritaires (classement + désinscription mails publicitaires). Vade Retro est numéro 1 en France en nombre de mailbox protégées (60M).