

SÉCURITÉ HUMAINE PAR LES MÉDIAS SOCIAUX :
NOUVEL ENJEU POUR LES ENTREPRISES

Secus

MAGAZINE
POUR LES ORGANISATIONS
ET LES GENS QUI S'INTÉRESSENT
À LA SÉCURITÉ INFORMATIQUE

(www.secus.ca)

LPRPDE :
MODIFICATIONS
ET OBLIGATIONS

LA SÉCURITÉ
À L'HEURE
DES AFFAIRES



La **fermeture** de l'**ISIQ** :
RAISONS ET CONSÉQUENCES

Nouvelle approche de détection des intrusions réseau

PAR **CHRISTOPHE BOY**,
cofondateur et président –
Altea Communications



Christophe Boy est cofondateur et président d'Altea Communications, une entreprise spécialisée dans l'intégration de solutions réseau et sécurité. Il a plus de quinze ans d'expérience dans les réseaux et la sécurité. Il possède de nombreuses certifications et collabore depuis des années avec Sourcefire (Snort), Rapid7 (Metasploit), Net Optics, Network Instruments, NetIQ, HPOV, etc.

Les réseaux actuels sont hautement dynamiques. Les menaces sont en constante évolution et deviennent de plus en plus sophistiquées. Les brèches au sein de la sécurité des réseaux continuent à se produire parce que les systèmes de défense statiques ne peuvent protéger les réseaux dynamiques actuels contre des menaces dynamiques.

Lorsqu'il s'agit d'assurer la sécurité de leur information, la plupart des entreprises d'aujourd'hui arrivent à peine à y parvenir. Malgré de lourds investissements, elles continuent de subir des brèches de sécurité et autres types d'incidents à un taux inacceptable.

Le principal problème est le changement dynamique des environnements à défendre, qui augmente le coût et la complexité des mécanismes de défense nécessaires et qui réduit l'efficacité de l'approche traditionnelle en sécurité, une approche reposant en grande partie sur un ensemble disparate de produits sans lien entre eux.

Plus particulièrement, parmi les changements et défis les plus importants auxquels font face les entreprises d'aujourd'hui qui dépendent de la technologie de l'information (TI), on compte un univers de menaces hautement dynamiques, un univers technologique en constante évolution et un univers réglementaire de plus en plus onéreux.

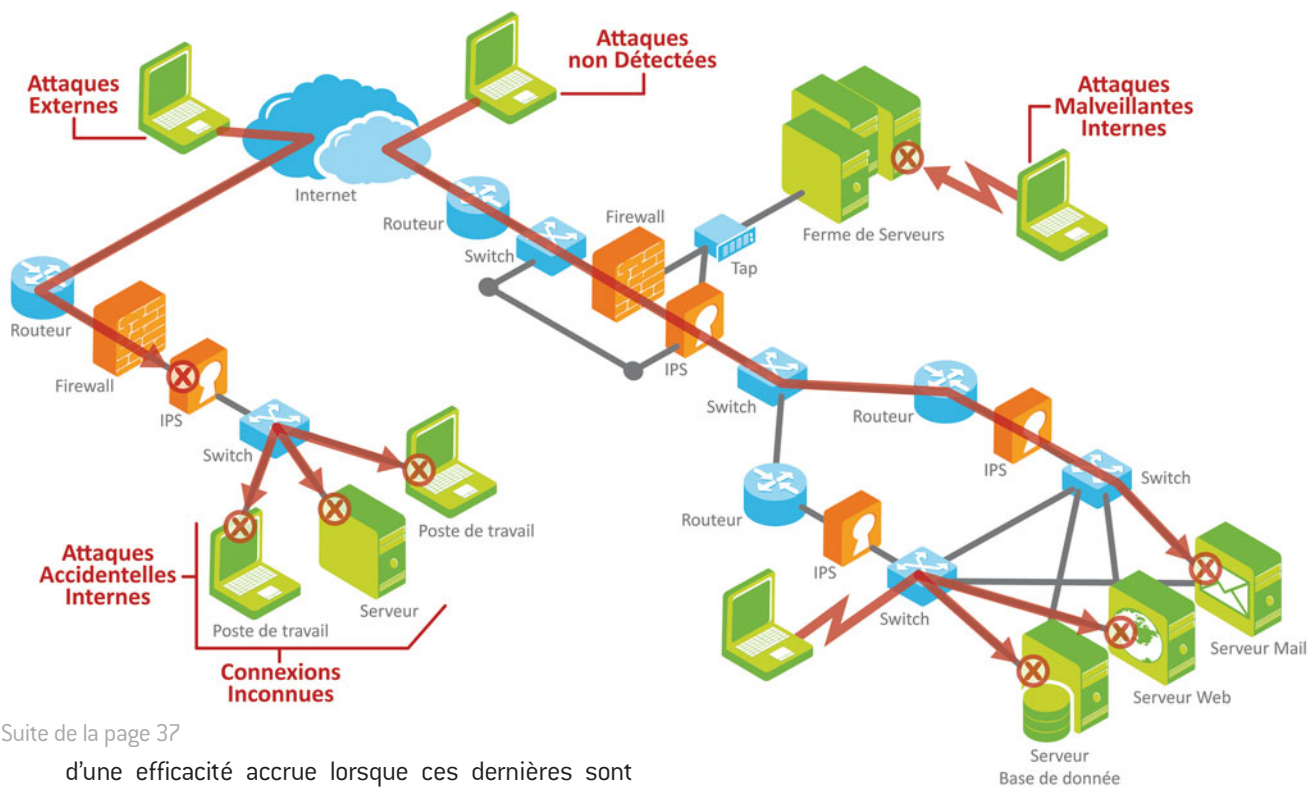
L'UNIVERS DES MENACES

Le temps où les entreprises ne faisaient face chaque année qu'à une poignée de virus sur le plan des serveurs et des postes clients et de vers de réseau est bien révolu. De nos jours, l'univers des menaces est beaucoup plus dynamique en raison d'un changement de motivation des pirates qui ne cherchent plus à gagner de la notoriété et à se bâtir une réputation, mais à s'enrichir.

Les changements particuliers et implications connexes d'une solution de sécurité d'entreprise comprennent les éléments suivants :

- La quantité de menaces à traiter dans une période donnée est en croissance. Les solutions de gestion doivent être plus efficaces.
- Les menaces sont produites plus rapidement que jamais. La période qui s'écoule entre l'annonce d'une nouvelle vulnérabilité et la divulgation d'un « exploit » correspondant n'est que de quelques jours, alors qu'elle se mesurait auparavant en semaines ou en mois. Avec aussi peu de temps pour réagir, l'efficacité des contre-mesures, notamment les outils antivirus et les systèmes de gestion de corrections, diminue, indiquant ainsi la nécessité d'y ajouter des mesures supplémentaires de nature plus proactive.
- Les menaces deviennent plus diversifiées. Les attaques par virus, vers et dénis de service de même que les réseaux de zombies (*botnet*) engendrant des milliers de courriels indésirables, les logiciels espions et les outils de dissimulation d'activité (*rootkits*) constituent une foule de techniques d'attaque de technologies et d'applications sur Internet. Par conséquent, les entreprises ont besoin non seulement d'un plus grand nombre de types de contre-mesures, mais

Suite en page 38



Suite de la page 37

d'une efficacit  accrue lorsque ces derni res sont exploiti es. Ou encore, les entreprises doivent avoir des contre-mesures capables de traiter de mani re inh rente les nouveaux types de menaces sans avoir   ajouter un nouveau produit.

- Les menaces deviennent plus  vasives. Des techniques telles que le camouflage (c'est- -dire l'utilisation de multiples m canismes de propagation ou d'exploit) et le ciblage (c'est- -dire la planification d'attaques personnalis es ciblant sp cifiquement une entreprise) ne font que confirmer la tendance g n rale d'une migration des menaces, une approche qui tire parti des faiblesses des applications pour s'infiltrer entre les d fenses.
- Les menaces viennent aussi de l'int rieur. Le fait de consid rer les menaces internes comme un « changement » est discutable. Plusieurs professionnels de la s curit  affirment en effet que les menaces internes sont non seulement pr sentes, mais qu'elles sont importantes et ont toujours exist . C'est le degr  de reconnaissance de la menace interne qui a chang  et mis l'accent sur des solutions de s curit  qui fournissent un examen plus minutieux des utilisateurs et syst mes internes et qui ne se limitent plus aux p rim tres et aux utilisateurs externes.

O  EN EST L'IPS (SYST ME DE PR VENTION D'INTRUSION) ?

Les fournisseurs d'IPS se vantent souvent du grand nombre de menaces qu'ils sont en mesure de d tecter et de la vitesse   laquelle ils cr ent les solutions capables de d tecter les nouvelles menaces. De nombreuses entreprises

sont pr tes   croire les yeux ferm s   ces arguments de vente, mais, en l'absence de preuves pour  tayer ces dires, il n'est pas certain qu'elles misent sur les bons chevaux.

UNE PROTECTION IMPOSSIBLE   V RIFIER

La plupart des fournisseurs d'IPS avancent des arguments qui n'ont fait l'objet d'aucun contr le et qui ne sont tout simplement pas v rifiables.

UNE PROTECTION PARTIELLE

La plupart des fournisseurs d'IPS offrent des solutions de protection qui ne concernent qu'un seul mode d'intrusion.

UNE PROTECTION QUI ARRIVE TROP TARD

La plupart des fournisseurs d'IPS ne proposent des solutions de protection qu'une fois les attaques survenues, connues du grand public et responsables d'importants dommages au sein de nombreuses entreprises.

UNE PROTECTION PEU FIABLE

La plupart des fournisseurs d'IPS utilisent des signatures qui ne r agissent pas parfaitement aux conditions de d clenchement d'une faille de s curit  et produisent par cons quent de faux positifs et de faux n gatifs.

Les pirates  tant de plus en plus habiles, les fournisseurs d'IPS se doivent de garantir une protection v rifiable :

- contre toutes les attaques possibles ;
- avant que de nouveaux modes d'intrusion n'apparaissent ;
- sans cr er de faux positifs ni de faux n gatifs.

Suite en page 39

LA SOLUTION : LES IPS ADAPTATIFS

La réponse à ces problématiques repose sur des systèmes de détection d'intrusion avant-gardistes, les IPS adaptatifs. Ils permettent une analyse plus détaillée et intelligente des différentes couches technologiques de l'entreprise.

Un tel système est capable de s'adapter automatiquement à l'environnement à défendre pour pouvoir réagir en temps réel aux modifications dynamiques de celui-ci. Il dresse une liste des vulnérabilités en temps réel et de façon passive, permettant entre autres une activation ou désactivation automatique des règles de protection. Ce système est donc capable de diminuer grandement les fausses alarmes tout simplement en corrélant les vulnérabilités et les attaques. Parmi les IPS adaptatifs, il y a la solution 3D de Sourcefire qui offre des options adaptées aux réelles menaces.

INTELLIGENCE RÉSEAU EN TEMPS RÉEL

La fonction Sourcefire RNA (Real-time Network Awareness) propose une intelligence réseau passive jour et nuit en gardant en mémoire un inventaire en temps réel des systèmes d'exploitation, des services, des applications, des protocoles et des vulnérabilités potentielles qui existent sur le réseau. RNA concentre cette intelligence de manière complètement passive tout en intégrant de manière transparente l'intelligence avec le système 3D.

La base de données hôte de RNA peut également être étoffée d'informations rassemblées par des outils de découverture actifs afin de développer davantage la richesse de l'intelligence réseau.

La combinaison de la visibilité réseau en temps réel de RNA avec Sourcefire RUA™ (Real-time User Awareness), une technologie qui lie l'identité de l'utilisateur à la sécurité et aux événements de conformité, donne une intelligence à l'échelle entière de l'organisation sur les réseaux dynamiques et les utilisateurs.

ÉVALUATION AUTOMATISÉE DE L'IMPACT

Les professionnels de la sécurité informatique (SI) n'ont pas le temps de filtrer chaque jour des centaines ou des milliers d'événements liés à la sécurité pour déceler l'événement le plus important. En tirant parti de l'intelligence réseau en temps réel de RNA de Sourcefire, les clients peuvent amener leur IPS Sourcefire au niveau suivant. La détection d'une attaque est automatiquement corrélée à la connaissance de la cible en temps réel de RNA pour déterminer la pertinence et l'impact d'une attaque. Grâce à l'évaluation automatisée de l'impact, les événements sont typiquement réduits de près de 99 %, ce qui permet aux administrateurs de se concentrer sur les événements qui nuisent véritablement aux réseaux.

RÉGLAGE IPS AUTOMATISÉ

Les professionnels de la SI ne peuvent pas constamment « régler » leurs IPS lorsqu'ils constatent un changement dans le réseau. En incorporant l'intelligence réseau en temps réel de la RNA à l'IPS Sourcefire, le processus continu du réglage de l'IPS peut également être automatisé.

Au fur et à mesure que le réseau évolue, les règles recommandées par la RNA évitent d'avoir à deviner comment déterminer quelles règles Snort activer et désactiver. La RNA recommande les règles Snort pertinentes en se basant sur le réseau qu'elle protège, et ces règles peuvent être activées avec ou sans intervention humaine. L'utilisation de la solution adaptative en temps réel de Sourcefire diminue la nécessité d'analyses manuelles des événements et du réglage de l'IPS par l'équipe responsable de la SI, réduit le potentiel d'interruption du réseau et constitue une économie en ce qui concerne les frais d'exploitation. En connaissant en temps réel ce qui se passe sur le réseau, le système 3D permet d'économiser du temps et de l'argent et maximise la protection du réseau en évolution constante.

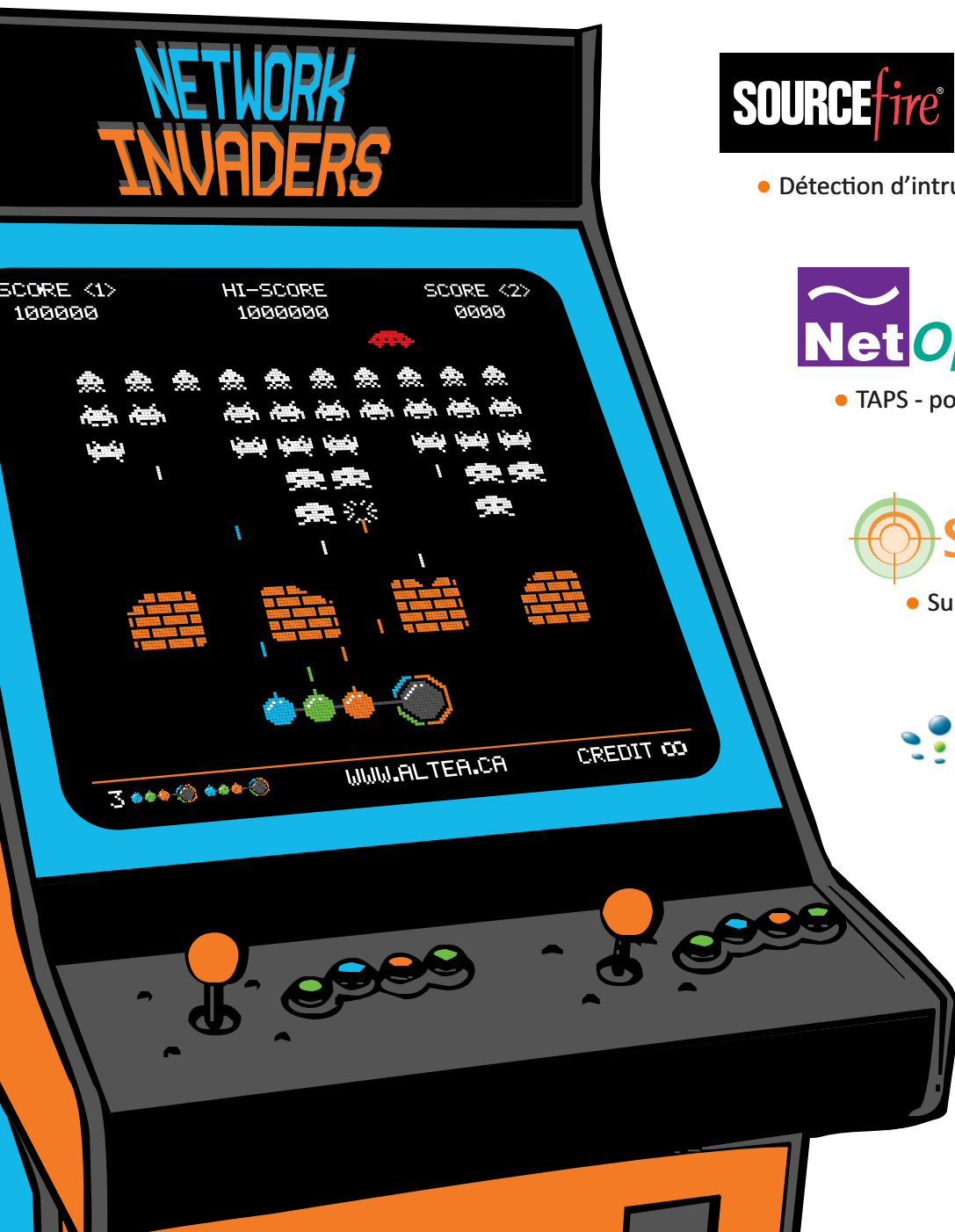
Dans un monde dynamique où le crime informatisé prend de plus en plus de place, les systèmes de détection d'intrusion protégeant les réseaux informatiques doivent être adaptatifs. Sans cette technologie, beaucoup d'efforts opérationnels sont nécessaires pour offrir une protection efficace. ■

**L'ANALYSE
DES GEEKS**

PODCAST HEBDOMADAIRE
SUR LES NOUVELLES
TECHNOLOGIES ANIMÉ
PAR **BEN LE GEEK**
ET **FRANK THE TANK.**

WWW.ANALYSEDES GEEKS.COM

PROTÉGER VOTRE RÉSEAU EST UN JEU D'ENFANTS POUR ALTEA GRÂCE À NOS PARTENAIRES :



- Détection d'intrusions



- TAPS - points d'accès pour test réseau



- Surveillance de l'activité des utilisateurs



- Analyse des vulnérabilités



- Gestion de la sécurité et de la conformité

Audits de sécurité • Tests de pénétration • Rédaction des normes de sécurité • Analyses «forensiques» • Déploiement de solutions • IPS/IDS • Pare-feu • TAPS (Points d'accès pour test réseau) • Impartition • etc.

Pour plus d'informations www.altea.ca

