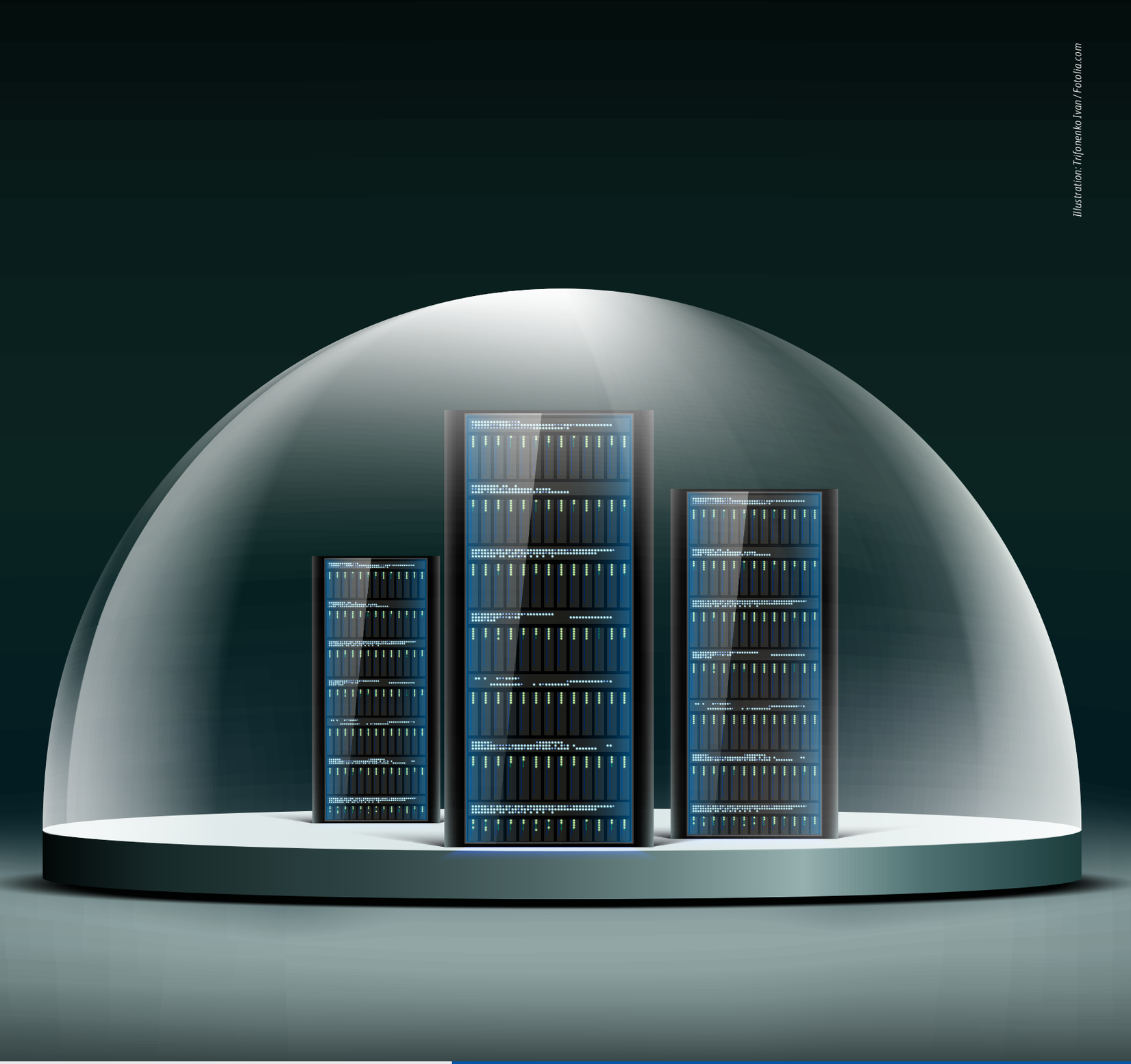


Illustration: Trifonenko Ivan / Fotolia.com

Dossier
Cybersécurité

en collaboration avec **Boll Engineering**

Un bouclier virtuel contre les attaques internet

osc. L'internet et le courrier électronique sont la porte d'entrée à toutes sortes de menaces pour les systèmes informatiques de l'entreprise. Ransomware, chevaux de Troie ou tentatives d'hameçonnage – le nombre et la sophistication des attaques du cyberespace sont en constante augmentation. En face, les fournisseurs de solutions de cybersécurité s'efforcent inlassablement de trouver des moyens de protéger les entreprises contre les menaces numériques.
La technique de «l'isolation» est une réponse dans cette recherche d'une plus grande sécurité. Elle consiste à isoler l'utilisateur d'un navigateur du contenu réel du web. Les sites ou les e-mails – y compris tout code malveillant – sont d'abord exécutés dans un environnement virtuel, puis transmis à l'utilisateur dans une version «nettoyée», sans scripts ni contenu Flash, promettent les fabricants. Patrick Michel et Roger Gomringer de Boll Engineering expliquent dans les pages qui suivent comment ce système fonctionne.

Combattre les cyber-menaces avec «l'isolation»

Les attaques zero-day et drive-by ne sont pas détectées par les solutions de sécurité conventionnelles et peuvent avoir des conséquences dramatiques. Grâce à «l'isolation» des utilisateurs face aux contenus préjudiciables, il est désormais possible de repousser complètement ces attaques – sans perte de vitesse ou de confort d'utilisation.

L'AUTEUR

Patrick Michel
Responsable des ventes
BOLL Engineering AG

Les dangers du cyberespace augmentent rapidement. Les attaques sont de plus en plus sophistiquées et complexes – et elles sont omniprésentes, comme le montre l'actuel State of the Web Report d'un fournisseur de solutions de sécurité. D'après cette étude, 44% des 100 000 principaux sites web indexés au Alexa Ranking ont été classés comme risqués, parce qu'ils propagent des logiciels malveillants, ont été récemment piratés ou parce qu'ils utilisent des logiciels dangereux.

En plus de visiter des sites web à risque, les attaques d'hameçonnage sophistiquées sont une source majeure de danger. Elles ciblent précisément les destinataires en s'adressant à eux par leur nom ou en employant d'autres détails personnels – on parle de «Spear Phishing» – et utilisent des services connus et populaires tels que les sites d'information et de voyage pour se propager. Les analystes de Gartner qualifient désormais Internet et tous ses services de véritable «cloaque d'attaques».

La détection ne suffit pas

Les architectures de cybersécurité conventionnelles sont basées sur le principe de la «détection». Les solutions antimalware détectent les modèles de logiciels malveillants connus et mettent en quarantaine le contenu concerné. En outre, des filtres web basés sur des listes noires bloquent l'accès aux sites dangereux. Le sandboxing est également basé sur la détection des logiciels malveillants. Le code à tester est exécuté dans un environnement protégé et classé comme dangereux ou non dangereux en fonction de son comportement.

La cyberdéfense basée sur la détection n'est qu'un moyen limité de repousser les méthodes d'attaque inconnues.

Aussi répandue qu'elle puisse être, la cyberdéfense basée sur la détection n'est qu'un moyen limité de repousser les méthodes d'attaque inconnues, qualifiées de «zero-day». Comme le prouve l'avènement des ransomwares, qui touchent un nombre incalculable d'utilisateurs malgré l'utilisation de solutions anti-malware sophistiquées.

De plus, la cyberdéfense purement basée sur la reconnaissance présente un autre inconvénient: non seulement elle bloque les codes malveillants, mais elle peut aussi avoir un impact négatif sur la productivité des employés. Les utilisateurs ne peuvent par exemple surfer sur le web que de manière limitée, puisque dans certaines entreprises, même les médias reconnus et les offres de médias sociaux sont bloqués.

Il faut une architecture conçue pour une «expérience utilisateur native».

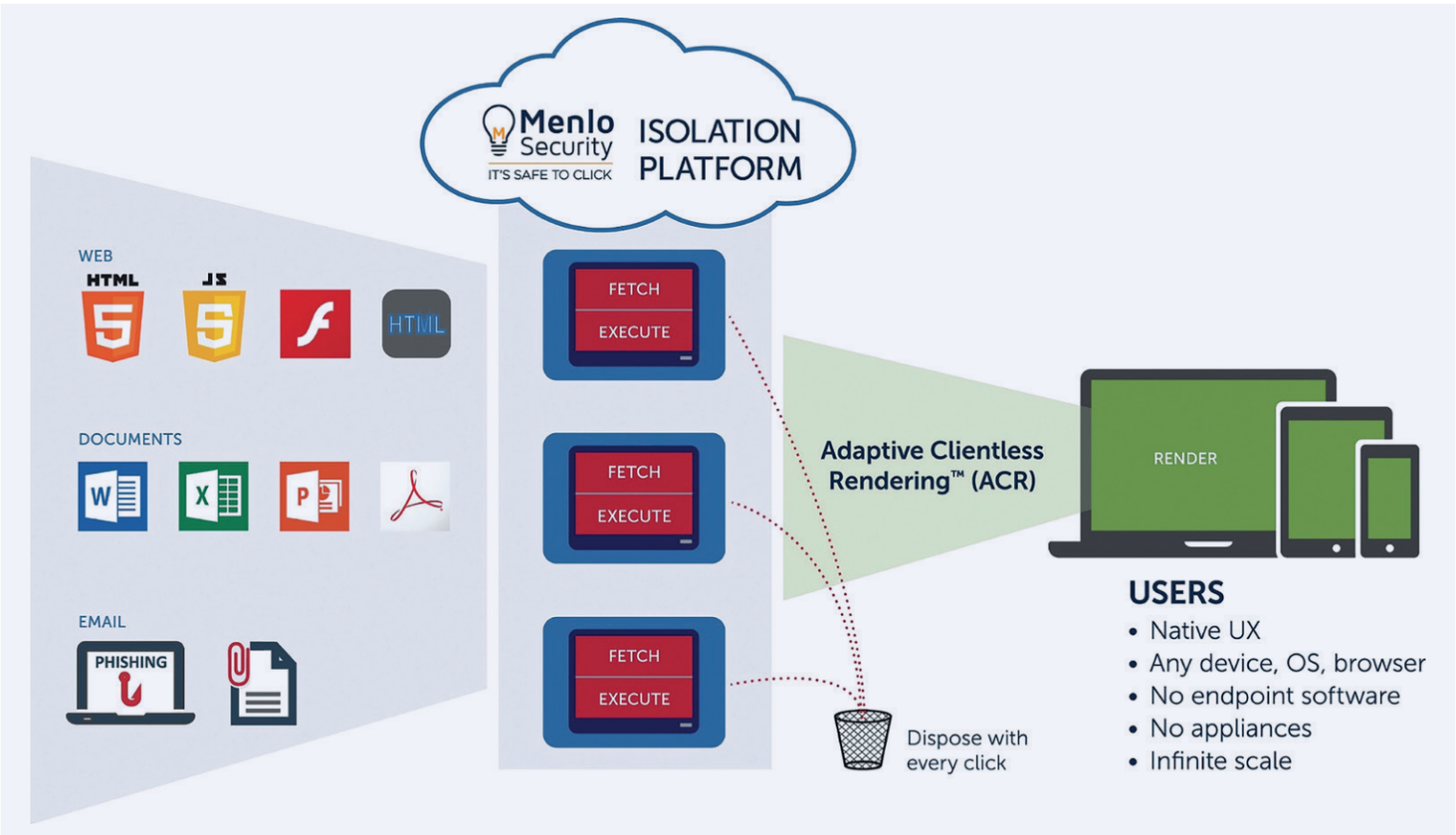
Le blocage de sites web individuels n'est pas sans raison, comme le montrent divers incidents en Suisse. En avril 2016, par exemple, un code malveillant a été distribué via une infection par drive-by sur 20minuten.ch – une publicité intégrée d'un réseau publicitaire était reliée à un site malveillant. Ce n'est pas surprenant étant donné le grand nombre de scripts et de de sites web tiers dont les contenus sont téléchargés. Si l'on examine la page d'accueil, on tombe sur 93 scripts et 25 sites chargés en arrière-plan – des valeurs typiques pour les nouvelles plateformes en ligne.

D'une manière générale, la sécurité et le business sont dans un dilemme. D'une part, tout ce qui est potentiellement dangereux est mis sur la liste noire du filtre web. D'autre part, les employés veulent un accès aussi libre que possible au web afin de ne pas être gênés dans leur travail. Il faut cependant garder à l'esprit que l'interdépendance croissante des sites web signifie qu'aucun site ne peut plus être considéré comme fiable. Pour cette raison, le filtrage web n'a qu'une utilité limitée du point de vue de la sécurité. Les catégories de filtres web pertinentes pour la sécurité ne couvrent qu'une fraction des sites dangereux, et le blocage de sites web individuels ou de catégories de sites nuit excessivement à la productivité des employés.

«L'isolation» apporte une défense forte

Gartner le proclame depuis 2016: «it's time to isolate». L'idée derrière tout cela: au lieu de bloquer complètement l'accès à un contenu spécifique, l'utilisateur est isolé de l'accès direct au web et ne reçoit que du contenu, des courriels et des documents sécurisés. Ainsi, une instance entre l'utilisateur et le site web dangereux prend en charge le travail à risque.

Les premières solutions de sécurité à base d'isolation sont déjà sur le marché. Certaines d'entre elles s'appuient simplement sur



une infrastructure de bureau virtuel (VDI). Le contenu original est récupéré et traité dans un environnement virtuel central – seul un flux vidéo est transmis à l'appareil de l'utilisateur. Cette solution garantit la sécurité, mais compromet le confort de l'utilisateur. En outre, les solutions basées sur VDI sont complexes et entraînent des coûts supplémentaires importants.

D'autres solutions placent l'environnement virtuel directement sur l'appareil final. Ce n'est pas vraiment pratique: si une machine virtuelle ou une instance de navigateur doit s'exécuter sur chaque PC des employés, les besoins en matériel et les efforts d'administration augmentent. En outre, les solutions correspondantes sont limitées à certains navigateurs et systèmes d'exploitation.

La plateforme d'isolation idéale

Pour obtenir une combinaison idéale d'isolation complète, conviviale et ne nécessitant qu'un faible effort d'administration, il faut une architecture conçue pour une «expérience utilisateur native», l'efficacité des ressources et l'évolutivité de l'entreprise. Ainsi, une plateforme d'isolation disponible sur le marché accepte les contenus web et exécute tous les codes actifs tels que Javascript et Flash dans un environnement virtuel isolé. Une infection possible se produit bel et bien, mais dans une «cage» d'où elle ne peut pas s'échapper. Les contenus originaux sont «éliminés» immédiatement après l'exécution. L'utilisateur ou son terminal reçoit une version rendue sans code actif. Les scripts ont été supprimés, les vidéos Flash sont automatiquement converties au format MP4.

Ce principe intelligent peut être utilisé non seulement pour le contenu web, mais aussi pour les documents et les courriels. De cette façon, les documents reçus sont analysés dans l'environnement isolé et transmis sous forme de prévisualisation sécurisée sans contenu actif. L'utilisateur peut également télécharger la version originale à ses propres risques. De plus, les e-mails sont scannés et les liens dangereux sont remplacés par des liens sécurisés pointant vers la plateforme d'isolation.

Avec la plateforme d'isolation décrite, aucun agent n'a besoin d'être installé sur l'appareil, l'utilisateur travaille avec son navigateur et son client de messagerie habituel. Il dispose de toutes les fonctionnalités. L'installation est également simple: la plateforme d'isolation fournit le contenu rendu via un service proxy. Sur l'appareil, il suffit de paramétrer le proxy. Dans un environnement géré, il est possible de gérer l'ensemble de manière centralisée via une URL de configuration. La plateforme d'isolation peut aussi être utilisée conjointement avec les solutions de proxy, de pare-feu et de filtrage web existantes et ajoute un niveau de sécurité supplémentaire. La plateforme est disponible à la fois en solution locale ou cloud.

L'expérience montre qu'une solution d'isolation conçue de cette manière prévient complètement les attaques zero-day et les attaques drive-by et n'entraîne aucune restriction perceptible ou perte de vitesse pour l'utilisateur. De larges installations avec plus de 100 000 utilisateurs prouvent que le concept s'adapte parfaitement aux environnements les plus vastes.

«L'isolation du navigateur est la technologie de cybersécurité du moment»

En entretien, Roger Gomringer, Business Development Manager chez le distributeur de sécurité informatique BOLL Engineering, parle du nouveau concept de sécurité que constitue «l'isolation», du développement du marché et de sa mise en œuvre la plus mûre et efficace à ce jour. Interview: Oliver Schneider

L'isolement est un concept relativement nouveau pour accroître la cybersécurité. Comment le marché évolue-t-il?
Le marché est encore limité à l'heure actuelle, mais il se développera fortement. Gartner prévoit qu'en 2021, la moitié du trafic web des entreprises sera isolée et considère l'isolation et les solutions de navigation à distance comme des technologies de pointe dans le domaine de la cybersécurité.

Est-ce que l'isolation est vraiment ce dont le client a besoin ou est-ce que tout cela n'est qu'une lubie des fabricants?
L'isolement est évidemment plus qu'un battage médiatique et touche un point sensible des entreprises. La banque américaine JPMorgan Chase s'appuie par exemple sur Menlo Security Isolation Platform pour désamorcer les sites web risqués et combattre le phishing qui arrive par le biais de liens dangereux dans les courriels.

Menlo Security promet 100% d'efficacité face aux logiciels malveillants. Comment faut-il le comprendre?
Les menaces web telles que les attaques drive-by sont empêchées à 100% par la plateforme Menlo, car les utilisateurs ne voient que du contenu inoffensif – même les meilleures solutions avancées de protection contre les menaces conventionnelles ne peuvent pas le faire. Lors de l'isolement des documents, Menlo en crée une version sécurisée. Ceux-ci sont libres de tout code actif et sont à la disposition de l'utilisateur pour un téléchargement sécurisé. Cependant un risque subsiste si l'entreprise permet que la version originale de ces documents soit mise à la disposition de l'utilisateur. Dans ce contexte, nous recommandons aux employés de suivre une formation supplémentaire sur l'hameçonnage et une sensibilisation à la sécurité.

Que faut-il d'autre que la plateforme Menlo pour minimiser davantage le risque?
Le service d'isolation du web et du courrier électronique peut être utilisé conjointement avec les technologies de sécurité traditionnelles, telles que les protections de messagerie et les proxys tout en leur ajoutant un facteur important: le vecteur d'attaque drive-by est entièrement couvert. Le service d'isolation de documents peut également être complété en option par un antivirus et un sandbox pour assurer la sécurité nécessaire lors du téléchargement des documents originaux.

«Les attaques drive-by sont empêchées à 100%»

Roger Gomringer, Business Development Manager chez BOLL Engineering

Quels segments de clientèle sont particulièrement visés?
La solution est utile dès 100 utilisateurs ou plus. Fondamentalement, nous nous adressons à toutes les organisations ou entreprises qui veulent offrir à leurs employés la plus grande liberté possible sur internet avec le plus haut niveau de sécurité possible. Les clients se trouvent dans des secteurs tels que la finance, l'assurance, l'industrie, les produits pharmaceutiques et le gouvernement.

Comment intégrer l'isolation dans les infrastructures existantes?
Du point de vue du réseau, la plateforme Menlo Security Isolation Platform fonctionne comme un proxy et peut être facilement intégrée dans le réseau de l'entreprise. En tant que solution cloud, elle ne nécessite aucune installation locale. Selon les besoins, une version sur site peut être implémentée avec tous les composants dans une seule machine virtuelle basée sur VMware ESXi ou dans une architecture multi-nœuds.

Entre le cloud et l'installation sur site, quelle est la variante la plus populaire en Suisse?
Il s'agit clairement de la variante sur site. Pour des segments de clientèle tels que les services financiers ou pharmaceutiques, il n'est pas question de transférer les données des utilisateurs vers une plateforme cloud hébergée à l'étranger. La plateforme cloud de Menlo est hébergée sur Amazon Web Services, au sein de la région AWS de Francfort pour les clients suisses.