VARS

Whitepaper

PROTECTION CONTRE LES INTRUSIONS POUR LES CABINETS JURIDIQUES

Propulsée par Cynet

Défis d'entreprise

Les cabinets juridiques reposent sur des informations qui sont désormais presque entièrement numérisées. Des informations personnelles et juridiques sensibles sont créées, consultées et partagées sur un ensemble d'appareils, notamment des ordinateurs de bureau, des ordinateurs portables, des tablettes et des téléphones intelligents. Les employés, les sous-traitants externes et les clients peuvent accéder aux systèmes du cabinet à tout moment, de pratiquement n'importe où. De plus en plus, et surtout depuis la pandémie de la Covid, les accès proviennent en majorité de l'extérieur du périmètre du réseau, ce qui étend l'accès à pratiquement n'importe quel endroit du monde où on dispose d'une connexion Wi-Fi.

Les appareils utilisés pour accéder aux données des cabinets juridiques sont souvent des appareils personnels, ce qui réduit le contrôle et augmente les risques. Comme de nombreux appareils peuvent contenir des données sensibles sur les clients, ils doivent être protégés des menaces, que ce soit au sein ou à l'extérieur du réseau de l'entreprise. Un accès frauduleux à un seul point d'accès pourrait entraîner une perte dévastatrice de données ou, pire encore, constituer un point d'entrée pour accéder à tout l'environnement de l'entreprise.

Les cabinets sont devenus des cibles très attrayantes pour les cybercriminels en raison de la grande valeur des informations juridiques, professionnelles, personnelles et financières qui y sont conservées. Plusieurs cabinets juridiques ont été victimes d'attaques par rançongiciels en 2020, comme celle perpétrée contre Seyfarth Shaw en octobre. Le rançongiciel a réussi à chiffrer les données de plusieurs systèmes et a contraint l'entreprise à fermer son service de messagerie et d'autres systèmes. Bien que le cabinet affirme qu'aucune donnée confidentielle n'a été volée, il a subi des perturbations et un impact potentiel à sa réputation. Les attaques par rançongiciels qui utilisent des techniques de crypto-verrouillage peuvent conduire à de longues périodes de recouvrement et à la perte de propriété intellectuelle.

Même les plus grands cabinets juridiques ont tendance à être soutenus par de équipes de cybersécurité réduites qui sont parfois également responsables du soutien informatique général. Avec pour principale responsabilité de maintenir le stockage des données et les systèmes des utilisateurs, le personnel chargé de la sécurité manque souvent de temps et d'expertise pour protéger correctement l'organisation contre les cybermenaces. Cette situation est particulièrement risquée dans un environnement hautement distribué et réparti entre plusieurs sites, avec une multitude d'appareils personnels, d'appareils appartenant à l'entreprise ou à des tiers, qui accèdent à distance au réseau de l'entreprise.

Principaux défis en matière de sécurité

Accès à distance largement distribué aux systèmes d'entreprise et à la propriété intellectuelle

De équipes de sécurité réduites qui disposent d'une expertise et de budgets limités en matière de technologies de cybersécurité

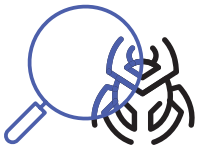
Le recours aux logiciels antivirus et de protection contre les logiciels malveillants traditionnels offre une protection limitée contre les menaces plus récentes telles que les rançongiciels et les attaques par crypto-verrouillage

> « Lorsque la pandémie de la Covid a éclaté, Cynet nous a permis d'étendre la protection à tous les points d'accès appartenant à des particuliers, sans frais supplémentaires. Cynet est un véritable partenaire. »
>
> CIO, Cabinet juridique

> « Il nous a littéralement fallu moins d'une semaine pour déployer et maîtriser la plateforme Cynet. La protection de l'entreprise n'est plus confuse ni chaotique. »
>
> CISO, Cabinet juridique

Principaux défis en matière de cybersécurité

La protection de l'environnement d'un cabinet juridique représente un défi en raison de son environnement largement distribué et de l'accès illimité aux actifs de l'entreprise depuis l'extérieur du périmètre du réseau. La protection des points d'accès à l'extérieur du réseau d'entreprise est particulièrement compliquée, notamment en raison du rythme d'échange d'informations propre au monde juridique. Un seul fichier malveillant infiltré dans un seul ordinateur portable pourrait entraîner des conséquences dévastatrices à l'échelle de l'entreprise.



Visibilité limitée sur l'ensemble de l'environnement

De nombreux cabinets juridiques ont recours à des logiciels antivirus et de protection contre les logiciels malveillants de base qui ne peuvent détecter qu'une fraction des attaques avancées. Ces logiciels offrent une protection limitée contre les nouvelles techniques d'attaque comme les rançongiciels et sont particulièrement vulnérables aux attaques ciblées très avancées. En définitive, même les meilleures techniques heuristiques ou de détection des logiciels malveillants basées sur les comportements ne peuvent pas détecter et prévenir 100% des menaces.

Pour étendre la protection au-delà des solutions d'antivirus, les entreprises ont recours à des outils supplémentaires tels que les outils de détection et d'intervention sur les points d'accès (EDR) et sur les réseaux (NDR). Les solutions EDR sont nées de la constatation que les menaces sont détectées une fois après avoir réussi à contourner un point d'accès, puisqu'un logiciel antivirus n'arrive pas à les anticiper. Les solutions EDR surveillent donc en permanence les points d'accès afin de détecter les activités malveillantes et les comportements du système qui indiqueraient une intrusion.

Les solutions NDR étendent la protection au réseau afin de fournir une visibilité supplémentaire sur l'ensemble de l'environnement. Si une attaque contourne d'une manière ou d'une autre un logiciel antivirus et une solution EDR, la possibilité de détecter les mouvements latéraux et d'autres indicateurs de trafic réseau pourrait permettre de découvrir un acteur menaçant qui a réussi à s'infiltrer dans l'environnement.

Finalement, la protection d'une variété d'appareils d'accès, de systèmes interconnectés et d'applications qui reposent sur une gamme de systèmes d'exploitation, de mises à jour et d'historique de correctifs constitue un défi pour les plus grandes entreprises mondiales. Les cabinets juridiques de petite et de moyenne taille sont confrontés aux mêmes risques, avec une fraction des ressources.

Dispositifs de contrôle de sécurité cloisonnés

Bien que chacun des contrôles de sécurité décrits précédemment améliore la visibilité nécessaire dans l'ensemble de l'environnement, ils ne sont pas sans inconvénient. Tout d'abord, les solutions EDR et NDR sont reconnues pour générer des fausses alertes. Les analystes de sécurité traquent celles-ci ou ont tendance à ignorer toutes les alertes, sauf celles qui semblent présenter les plus grands risques. Dans le premier cas, les analystes perdent un temps considérable. Dans le second cas, ignorer des alertes est contraire aux bonnes pratiques de sécurité et expose l'entreprise à des risques d'intrusion.

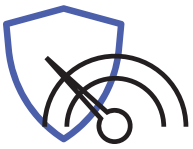
Principaux défis en matière de cybersécurité

(suite)

Dispositifs de contrôle de sécurité cloisonnés

(suite)

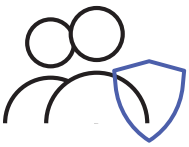
Les dispositifs de contrôle cloisonnés signifient également que l'équipe de sécurité doit surveiller et accéder à un plus grand nombre de « tableaux de bord » lorsqu'elle examine des menaces potentielles. Comme chaque outil de sécurité dispose d'une console de gestion distincte et présente les informations différemment, il est difficile pour les analystes de sécurité de donner un sens à toutes les informations présentées, puis de lier les activités entre les différents contrôles de sécurité pour avoir une vue d'ensemble. C'est pourquoi les attaques furtives sont capables de contourner les environnements dotés de plusieurs niveaux de contrôle.



Des équipes de sécurité réduites avec des ressources limitées

Si l'on met de côté les dispositifs de contrôle cloisonnés, lesquels impliquent plusieurs manipulations, la plupart des outils de sécurité nécessitent un investissement humain significatif pour fonctionner. Lorsque des menaces sont découvertes, les analystes en sécurité doivent investiguer pour en déterminer la cause, puis découvrir l'étendue complète de l'attaque dans l'ensemble de l'environnement.

Une fois la cause et l'étendue de la menace déterminées, il faut remédier à toutes les composantes de celle-ci. Cela implique souvent d'accéder à plusieurs systèmes, ce qui peut s'avérer un processus long et fastidieux.



Des équipes de sécurité réduites avec une expertise limitée en matière de cybersécurité

Avec l'évolution rapide du spectre des menaces, même les équipes de sécurité les plus importantes et les mieux financées sont vulnérables envers celles-ci. Il suffit d'étudier les intrusions commises dans les grandes entreprises pour se rendre compte que même les meilleurs experts en cybersécurité, dotés d'outils de pointe, ont du mal à protéger leurs organisations. Pour les équipes de sécurité réduites qui disposent de budgets technologiques et d'une expertise en cybersécurité limités, le risque d'intrusion augmente de façon exponentielle.

L’approche Cynet-VARS

Cynet a été conçu pour les équipes de cybersécurité réduites dont les ressources, l’expertise en cybersécurité et les budgets technologiques sont limités. Cynet XDR fournit une plateforme unique et unifiée pour prévenir et détecter automatiquement les vecteurs d’attaque auxquels sont confrontées les cabinets juridiques, investiguer sur ceux-ci et y remédier. La visibilité sur les points d’accès, les réseaux et les activités des utilisateurs, ainsi que la puissance de la simulation de ressources, offrent la protection la plus élargie et la plus approfondie contre toutes les menaces.

Cynet XDR est la seule solution qui déclenche une investigation automatisée à la suite de chaque alerte quant aux points d’accès, aux utilisateurs ou aux réseaux, en dévoilant entièrement la cause et la portée de l’alerte et en appliquant toutes les mesures correctives nécessaires pour éliminer complètement la menace. Cynet offre également un large éventail d’actions correctives automatisées et pouvant être personnalisées pour traiter les incidents en fonction de vos préférences. De plus, Cynet offre les services d’une équipe d’experts en cybersécurité pour renforcer et guider votre équipe 24 heures sur 24, 7 jours sur 7. Cette offre est incluse dans la plateforme Cynet 360.

Les avantages de Cynet pour les cabinets juridiques

Facile à déployer et à exploiter

L’agent Cynet peut être déployé sur plus de 5 000 points d’accès en moins d’une heure. Alors que de nombreuses solutions nécessitent des mois pour être déployées et devenir pleinement fonctionnelles, Cynet est prêt dans les 24 heures suivant le déploiement et fournit toutes les informations et protections disponibles dans la plateforme. La console Cynet a été conçue pour être intuitive et sans effort, de sorte que les petites équipes de sécurité n’ont pas besoin de plusieurs années d’expertise pour l’utiliser.

Visibilité totale dès la première utilisation

Cynet XDR offre une visibilité complète et de multiples points de télémétrie, ce qui permet de réduire les faux positifs et de détecter rapidement les menaces furtives. Une plateforme unique et unifiée de détection et d’intervention étendues (XDR) fournit un antivirus de nouvelle génération (NGAV), la détection et l’intervention sur les points d’accès (EDR), la détection et l’intervention sur le réseau (NDR), une analyse du comportement des utilisateurs et des entités (UEBA) et une technologie de simulation, le tout entièrement intégré et facilement configurable avec le tableau de bord unique qui est inclus.

Les avantages de Cynet pour les cabinets juridiques

(suite)

Protection automatisée

L'*Incident Engine* de Cynet effectue automatiquement toutes les investigations sur les menaces et les mesures d'intervention requises, en identifiant la cause fondamentale et la portée complète des menaces à haut risque et en prenant les mesures appropriées pour éradiquer complètement la menace dans l'ensemble de l'environnement. Cynet offre en outre une liste de stratégies qui peuvent être exécutées automatiquement en réponse à une menace détectée pour une intervention immédiate ou qui peuvent être déclenchées manuellement pour fournir plus de supervision et de contrôle. Les actions d'intervention autonomes de Cynet offrent la protection complète que les petites équipes de sécurité surchargées recherchent.

Supervision de la détection et des interventions gérées incluse

Tous les clients de Cynet sont automatiquement protégés par un service complet de détection et d'interventions gérées (MDR), lequel est inclus dans la plateforme Cynet sans frais supplémentaires. Les petites équipes de sécurité des entreprises de ce secteur peuvent compter sur l'équipe MDR de Cynet (CyOps) pour surveiller de façon proactive leur environnement 24 heures sur 24, 7 jours sur 7, afin de s'assurer que rien n'est négligé. Elles peuvent contacter VARS tout moment pour obtenir des conseils sur la configuration de la plateforme Cynet. CyOps leur offre une expertise en matière d'investigation des attaques et les guide dans toutes les interventions nécessaires. CyOps devient un prolongement de l'équipe de sécurité pour un cabinet, ajoutant des ressources et une expertise de classe mondiale en matière de cybersécurité.

Résumé

Protéger les cabinets juridiques contre les cyberattaques représente un véritable défi, surtout avec une équipe de sécurité réduite et moins expérimentée. Avec des budgets limités, la plupart des cabinets juridiques de petite et de moyenne taille ne peuvent pas obtenir, intégrer et exploiter les contrôles de sécurité nécessaires pour protéger l'organisation contre les menaces avancées. Les cabinets juridiques peuvent compter sur la plateforme intuitive et complète de protection contre les intrusions de Cynet pour résoudre leurs enjeux de sécurité, en sachant qu'ils bénéficient toujours d'une équipe d'experts en cybersécurité pour les appuyer.