Top 6 des tendances en matière de cybersécurité - 2021

Services GRC

Rapport technique

Préparé par l'équipe GRC

24 janv.2021

Gestion de documents

Informations sur le document			
Directeur de projet:		Numéro de projet:	
Chef de projet:		Numéro SOW:	
Nom du projet:		Date de début du projet:	
Nom de la compagnie:		Date d'achèvement:	

Version du document	Date	Auteur	Noter
0,1	24 janv.2021	Tarun Chandola	Brouillon

Table des matières

Résumé

B&R s'engage à assister ses clients dans la création, l'adoption et la mise en œuvre d'un programme de gouvernance de la sécurité de l'information conçu pour protéger la confidentialité, l'intégrité et la disponibilité des informations confidentielles. B&R reconnaît l'obligation d'être conscient de l'évolution de toutes les tendances importantes de l'écosphère de cybersécurité.

Fond

B&R est l'un des principaux fournisseurs de solutions de cybersécurité avec des clients stratégiques.

Basé sur l'histoire de B&R et la place actuelle de l'industrie de la cybersécurité, il est évident que la disponibilité, l'intégrité et la confidentialité des données critiques et la connaissance de l'évolution de toutes les menaces pesant sur les données sensibles sont vitales pour notre entreprise. Consciente de ces risques, l'équipe GRC a effectué une analyse des tendances actuelles en matière de cybersécurité afin que nous puissions construire et proposer des stratégies de protection des informations appropriées à nos clients.

Méthodologie et approche

L'analyse des tendances en matière de cybersécurité de l'équipe B&R GRC a utilisé trois phases dans son évaluation.

B&R GRC Méthodologie d'évaluation

Top 6 des tendances en matière de cybersécurité

Le paysage des menaces de cybersécurité est une écosphère dynamique qui ne cesse d'évoluer. Il est important de connaître les principales tendances en matière de sécurité pour être mieux armé dans notre guerre contre la cybercriminalité.

Un examen totalement honnête des tendances en matière de sécurité est difficile pour les trois raisons suivantes:

1. Les entités commerciales sont toujours tentées de passer les incidents sous le tapis en les qualifiant de comportement anormal ou en jouant à un jeu sémantique. Dans certains cas, la loi est de leur côté, par exemple, les violations de la loi HIPAA ne doivent être signalées que si plus de 500 enregistrements sont divulgués.
2. Applications mal configures, comme Splunk. La plupart des organisations ont acheté des outils complexes de gestion de la cybercriminalité pour la gestion des journaux comme Splunk sans se rendre compte que ces outils complexes nécessitent une équipe qualifiée pour être configurés et maintenus. En conséquence, un grand nombre d'outils de surveillance des journaux de cybersécurité se sont révélés insuffisamment configurés, ce qui entraîne des lacunes dans la surveillance des activités suspectes.
3. Les cybercriminels vraiment intelligents ont une empreinte numérique minimale pour la criminalistique. Les cyberattaques les plus réussies sont celles qui peuvent être encore en cours et certaines peuvent ne jamais être identifiées comme le vol de bitcoins.

. Voici cinq tendances intéressantes à partir de 2020 qui aideront à mieux gérer les risques.

Tendance 1: Les incidents vont augmenter, qui surveille les observateurs ?

Quoi: SolarWinds est comparé à Microsoft avec lequel il est en concurrence et propose des produits qui sont utilisés dans la plupart des sociétés “Fortune 500” pour la numérisation de réseau.

La société, avec l'aide de KPMG et de Crowdstrike, a découvert un “code très sophistiqué et nouveau” qui a injecté le malware Sunburst dans les produits Orion, selon un Article de blog du 11 janvier, du président et chef de la direction de SolarWinds, Sudhakar Ramakrishna.

Le code d'injection - que CrowdStrike appelle Sunspot - insère Sunburst dans les versions logicielles en remplaçant un fichier source. CrowdStrike a déclaré que les attaquants avaient pris des mesures de protection pour s'assurer de rester à l'écart du radar des développeurs de SolarWinds. (Pour plus de détails techniques,lire le message de CrowdStrike.)

Comment : Les chercheurs en sécurité de Kaspersky ont partagé leurs découvertes détaillant “plusieurs caractéristiques qui chevauchent une porte dérobée précédemment identifiée connue sous le nom de Kazuar”, qui a été identifiée pour la première fois par les chercheurs de Palo Alto en 2017.

Les chercheurs de Kaspersky - et d'autres, comme Palo Alto - notent que l'outil Kazuar est souvent utilisé par Turla, groupe russe de menaces persistantes avancées, ou APT.

Les clients de Solarwinds ont été exposés dans le hack SolarWind par conséquent vont de Boeng à scanner leurs réseaux, y compris les entrepreneurs sensibles de la défense et un certain nombre d'agences fédérales très sensibles du ministère de la Justice

le gouvernement américain a reconnu les rapports d'infractions du département du Trésor américain et de l'administration nationale des télécommunications et de l'information du département du Commerce.

RCA : Il s'agit d'une tempête parfaite de hacking parrainé par l'État (SSH), d'outils sophistiqués et de l'utilisation de mots de passe par des pirates informatiques.

Analyse détaillée:

Environ 345 000 vulnérabilités sont identifiées chaque jour. La plupart sont pris en compte par les différents outils de lutte contre la cybercriminalité et les outils de sécurité réseau comme les pare-feu IDS, Anti-virus, SIEM et incorporés sous forme de signatures. Cela amène les pirates à relever le défi d'exploiter la vulnérabilité en plaçant ce malware pour infecter le réseau victime.

C'est un pur génie d'utiliser les outils de cybersécurité pour infecter le client, car chaque réseau est obligé de faire confiance et d'accepter le trafic et les paquets circulant vers leur environnement sécurisé en provenance du fournisseur d'assurance de sécurité de confiance.

Nous devrions nous attendre à ce que d'autres groupes de piratage sponsorisés par l'État essaient de pénétrer davantage dans les entreprises offrant davantage de solutions de sécurité. En fait, certains mettent déjà en garde contre les menaces d'inclure des intrusions dans Microsoft 365 et l'environnement cloud Azure, même sans l'utilisation de logiciels malveillants implantés dans SolarWinds.

Résolution et recommandations possibles:

- Contrôle plus strict de l'accès au code source des outils de sécurité pour fournir un niveau d'intégrité plus élevé dans les mises à jour des outils de sécurité.
- Test possible dans le bac à sable des signatures de mise à jour des outils de sécurité. Cela peut être contre-productif car le modèle actuel de mise à jour de confiance est universellement accepté.

Tendance 2: Croissance des ransomwares + 299% de croissance et 11,5 milliards de pertes

En 2019, Sonicwall vient de signaler une croissance de 299% des ransomwares d'une année sur l'autre. PDG d'un fournisseur de services anti-hameçonnage appelé Ransomware the new Normal.

Les coûts globaux des dommages liés aux attaques de ransomwares devraient atteindre11,5 milliards de dollars par an d'ici 2019

Comment: Le ransomware est conçu pour crypter totalement le système de fichiers d'une victime, provoquant une perte irréversible d'accès aux données sensibles. Ce type de cyber extorsion devient de plus en plus populaire parmi les criminels, car les victimes sont parfois disposées à débourser des millions de dollars pour déchiffrer leurs données.

RCA: La menace des ransomwares augmente car il est facile d'infecter les systèmes des petites et moyennes entreprises en exploitant des tactiques de phishing et pratiquement impunis car les criminels se cachent derrière des paiements en bitcoins et peuvent peut-être mener de telles activités criminelles à partir de pays où de telles activités ne sont pas considérées comme illégales par les autorités locales. Les petites et moyennes entreprises dont les processus sont critiques, telles que les hôpitaux et les administrations municipales, continuent à être confrontées à un risque plus important.

Résolution et recommandations possibles:

Étant donné que 91% des cyberattaques liées à une infection par ransomware ont été lancées avec des e-mails de spear phishing, les entreprises doivent installer des contrôles anti-hameçonnage ainsi qu'une formation des utilisateurs finaux.

- Sauvegardes adéquates avec BCP et DRP.
- Cyberassurance pour récupérer les pertes commerciales.

Tendance 3: l'IA doit être armée pour la cybercriminalité en combinaison avec l'IOT.

Les progrès de l'IA donneront aux cybercriminels la capacité d'exploiter les vulnérabilités IOT pour mener non seulement les attaques DOS standard avec BOTS, mais aussi pour arnaquer en utilisant la présence des joueurs et des victimes sur les réseaux sociaux.

Un logiciel basé sur l'IA a récemment été utilisé par des criminels pour deepfake afin de reproduire la voix d'un PDG pour commander un transfert d'argent de 243 000 $. Le chef de la société d'énergie a été victime d'une arnaque en pensant qu'il parlait au téléphone avec son patron qui lui a demandé d'effectuer le paiement. La fausse voix du patron a ordonné au chef d'envoyer de l'argent de toute urgence à une entreprise hongroise dans l'heure.

La croissance du nombre d'appareils connectés au net, Internet des objets (IoT) est une aubaine pour les cybercriminels. Un criminel peut accéder et exploiter le réseau via des appareils ou contrôler tous les composants des réseaux industriels d'une manière sans précédent. Tout, des pompes des stations-service aux réacteurs nucléaires, est de plus en plus exposé à de telles cybermenaces.

Il y a un incident célèbre où un dispositif de surveillance d'aquarium qui a été utilisé pour pirater un système de casino pour avoir commis un cyber-braquage d'un million de dollars. De telles attaques utilisant des appareils IOT se multiplient.

RCA : Tout appareil connecté qui n'est pas correctement sécurisé (ou pas du tout sécurisé) fonctionne comme une faille dans l'armure de cyberdéfense, exposant l'ensemble de l'environnement de cyberdéfense. Les appareils peuvent être utilisés pour des attaques de déni de service distribuées, avec des méchants les recrutant dans leurs efforts pour surcharger les services en ligne ou être utilisés en conjonction avec l'IA pour la puissance de traitement pour attaquer d'autres infrastructures.

Résolution et recommandations possibles:

- Identifiez et créez un inventaire de tous les appareils IOT (tout appareil avec une adresse IP et avec une connectivité) et gérez de manière adequate, en vous concentrant sur tous les contrôles de sécurité d'informations comme la gestion des accès et la mise à jour des correctifs.

Tendance 4: Augmentation de Piratage sponsorisé par l'État et APT

Les pirates nord-coréens se sont avérés être les maîtres d'œuvre des attaques du réseau SWIFT contre les banques pour avoir volé des millions de dollars et d'autres pour des attaques de cyberguerre comme le sabotage, l'exploitation et le vol de données. L'ONU estime que le pays a volé environ 2 milliards de dollars par le biais de cyberattaques "généralisées et de plus en plus sophistiquées". L'argent volé par la cybercriminalité est utilisé pour financer le développement de programmes d'armes de destruction massive.

La Russie est considérée par les experts comme le principal coupable du récent piratage de SolarWinds. (Voir Tendance 1)

RCA : On s'attend à ce que le piratage informatique parrainé par l'État avec la menace persistante avancée se développe pour des raisons politiques et en raison du manque de contrôle d'un gouvernement sur un autre. La cyberguerre devrait devenir plus violente dans les années à venir car les enjeux ne cessent de croître avec une dépendance de plus en plus grande aux ordinateurs.

Résolution et recommandations possibles:

- Masquez si possible vos activités pour ne pas être sur les radars des hackers.

- Mettre en œuvre la gouvernance de la cybersécurité en mettant l'accent sur la maturité de tous les processus de sécurité.
- Alignez-vous sur un programme de conformité accepté et reconnu comme NIST, PCI, ISO 27001.

Tendance 5: En moyenne plus de 6 mois de fuite de données avant d'être découvert

Selon Ponemon Institute au nom d'IBM, le nombre de jours avant qu'une faille ne soit découverte est maintenant de 197 jours, ce qui entraîne plus de 6 mois de fuite de données ininterrompue pour les pirates informatiques. Les entreprises qui ont pu contenir une brèche en moins de 30 jours ont économisé plus de 1 million de dollars par rapport à celles qui ont pris plus de 30 jours (3,09 millions de dollars contre 4,25 millions de dollars en moyenne).

RCA : Les lacunes dans la gestion des processus de sécurité et le manque d'harmonie entre les personnes, les processus et les technologies exposent l'organisation à des incidents de cybersécurité mais aussi à un retard dans la détection des processus suspects.

Résolution et recommandations possibles:

- Identifiez les lacunes dans la surveillance des activités suspectes anormales de votre environnement sensible et mettez en œuvre un plan SIEM solide et mature.

Tendance 6: Crypto jacking croissance de 34 000% sur l'année

En moins d'un an, le cour du Bitcoin a augmenté de plus de mille pour cent. Ce boom de la crypto-monnaie conduit à l'extraction de bitcoins et au cryptojacking de 34 000%.

La menace est si nouvelle que de nombreuses entreprises ne savent même pas que la puissance de calcul de leurs systèmes est volée.

L'extraction de pièces de monnaie pour la crypto-monnaie nécessite beaucoup de puissance de calcul. Les mineurs de pièces tentent d'infecter vos systèmes et de détourner la puissance de traitement de leur calcul cryptographique.

L'extraction de pièces de monnaie entraîne un ralentissement des appareils, une surchauffe des batteries et, dans certains cas, une panne de circuit.

Les réseaux d'entreprise risquent d'être facturés pour l'énorme utilisation du processeur cloud et la consommation d'énergie

L'extraction de pièces de monnaie est si rentable et si facile que des millions de sites web sont compromis pour accéder aux appareils des utilisateurs pour l'extraction. Actuellement, plus d'un milliard d'appareils seraient concernés par l'exploitation minière sur le web. Les appareils sont également piratés de manière à ce que 100 % de leur puissance de traitement puisse être volée,

ce qui entraîne une surchauffe des circuits informatiques et, à terme, leur épuisement. L'un des moyens novateurs par lesquels les mineurs ont pu gagner des Bitcoin a été de compromettre les réseaux Wi-Fi publics. Le réseau WiFi d'un café de Buenos Aires a été infecté par un logiciel malveillant qui a provoqué un retard de 10 secondes lors de la connexion au réseau. Les auteurs du malware ont ensuite exploité les ordinateurs portables des utilisateurs pour la cryptographie minière.

RCA: Les cybercriminels continueront à trouver des moyens innovants pour voler des ressources, car ces crimes sont souvent impunis et difficiles à poursuivre légalement.

Résolution et recommandations possibles:

- Pratiquez la cyberhygiène sur tous les environnements avec une gestion adéquate des patch