VECTRA®

Six vecteurs d'attaque critiques à détecter dans vos centres de données et votre cloud privé

La segmentation a fait son temps

La sécurité des centres de données et des environnements virtualisés est conçue à l'image de la sécurité du réseau de campus classique. En prenant comme modèle le périmètre réseau, les entreprises du secteur se sont d'abord attachées à recréer des fonctionnalités similaires à celles d'un pare-feu pour segmenter le flux de trafic au sein du centre de données virtuel et lui appliquer des règles.

Dans un premier temps, elles se sont contentées d'adapter les pare-feux traditionnels pour qu'ils s'exécutent comme des machines virtuelles, avant de passer à des modèles de segmentation avec agents et étroitement intégrés avec le logiciel de plate-forme de virtualisation lui-même. Les deux approches se concentrent essentiellement sur la manière d'appliquer les stratégies au sein du centre de données hébergé dans le cloud.

Toutefois, la création et l'application de règles sont loin de suffire pour détecter les cyberattaques. Au niveau du périmètre, la protection par pare-feu a été renforcée par une série de technologies de détection et de prévention des menaces, notamment des solutions IDS/IPS, antimalware ou encore de filtrage web.

À l'instar des pare-feux, bon nombre de ces technologies périmétriques de prévention des menaces ont été simplement ajustées pour s'exécuter sur des machines virtuelles, afin d'obtenir une réplique de l'architecture de sécurité d'un réseau de campus.

Malheureusement, les centres de données dans le cloud ne peuvent se limiter à une version améliorée de la sécurité du périmètre réseau. Ils sont en effet souvent confrontés à des cybermenaces à un stade plus avancé de l'attaque que le périmètre et donc à des types de menaces et des techniques d'attaque différents.

Plus précisément, la prévention des menaces au niveau du périmètre réseau consiste essentiellement à détecter la compromission ou infection initiale (par ex. les exploits et les malwares). En revanche, la cybersécurité d'un centre de données cloud doit se concentrer sur la détection des cyberpirates qui ont déjà compromis les défenses périmétriques et sont passés aux phases suivantes de l'attaque, notamment la reconnaissance interne, le déplacement latéral et l'exfiltration de données.

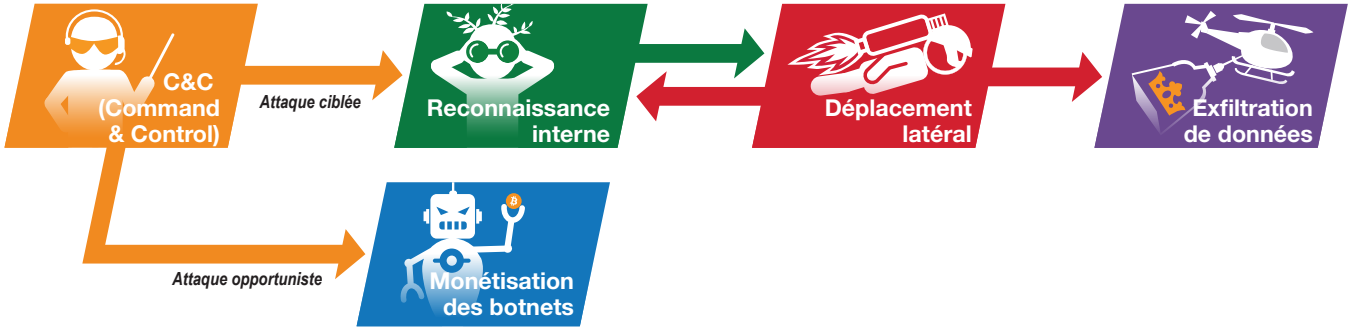
Il faut donc une approche de cybersécurité d'un nouveau genre, axée sur les activités internes d'un réseau. Celle-ci doit s'appuyer sur des modèles de détection fondés sur l'intelligence artificielle, l'apprentissage automatique et l'analyse comportementale pour débusquer les cyberpirates qui ont déjà établi une présence leur conférant des privilèges dans le réseau.

Une telle approche de la détection des attaques, c'est-à-dire axée sur « l'intérieur » du réseau, est encore plus importante dans le centre de données cloud. Bien avant d'accéder à une charge de travail virtuelle, le cyberpirate a déjà compromis le périmètre réseau et l'équipement d'un utilisateur final, et volé des identifiants d'administration.

Au lieu de bombarder directement les ressources du centre de données d'exploits ou de charges actives malveillantes, l'auteur de l'attaque préfère généralement profiter de ses privilèges pour mettre la main sur des ressources critiques ou les détruire.

La conception de la sécurité du centre de données cloud à l'image de la protection du réseau de campus a conduit à un « vide sécuritaire » dans le centre de données. Alors que le secteur n'a pas ménagé ses efforts pour intégrer la segmentation et l'application native de stratégies au réseau virtualisé, il a très peu investi dans l'innovation en matière de détection des menaces au sein des réseaux virtuels.

Pire encore, les modèles traditionnels de prévention des intrusions au niveau du périmètre ne sont pas conçus pour détecter les attaques évoluées auxquelles les centres de données sont actuellement exposés. Il est impératif d'adopter un nouveau modèle capable d'intégrer la cybersécurité à l'environnement virtualisé natif du centre de données dans le cloud.



Phases d'une cyberattaque au sein d'une chaîne de frappe

Intégration native avec l'environnement virtualisé

En plus de détecter les phases avancées d'une attaque, la cybersécurité du centre de données doit être intégrée de façon native avec la plate-forme de virtualisation. Une analyse des centres de données dans le cloud révèle que 80 % du trafic reste à l'intérieur du centre de données. Fondamentalement, la solution de sécurité doit être installée au sein de la plate-forme virtuelle pour offrir une visibilité sur les menaces potentielles.

Toutefois, incorporer la cybersécurité à la plate-forme de virtualisation ne suffit pas. L'environnement virtuel est toujours en mouvement. La nature agile et dynamique de la virtualisation est l'une de ses qualités les plus intéressantes.

Les développeurs peuvent rapidement inventer de nouvelles applications. À mesure que les besoins évoluent, les applications peuvent être facilement déplacées ailleurs, parfois sur un système physique totalement différent.

Pour être en mesure d'identifier des comportements malveillants et la progression d'une attaque, la solution de sécurité doit pouvoir bénéficier du contexte et d'une visibilité sur tous ces changements apportés à l'environnement virtuel. Dès lors, exécuter une application de sécurité sur un système quelconque de l'environnement virtuel ne suffit pas.

Cette visibilité et ce contexte doivent être obtenus en mode natif sur la plate-forme virtualisée elle-même. Au lieu d'être une simple pièce sur l'échiquier virtuel, la solution de sécurité doit en être la tête pensante et avoir une vision d'ensemble de l'évolution de toutes les pièces et du contexte au fil du temps. Sans ce contexte, il est tout simplement impossible de modéliser les comportements.

Visibilité unifiée pour toutes les équipes

Outre la détection des attaques actives, la solution doit assurer à toutes les équipes opérationnelles une visibilité unifiée sur la sécurité du centre de données. En effet, un centre de données dans le cloud n'est pas géré par une seule équipe mais par plusieurs, chacune ayant ses propres priorités et calendriers.

Les développeurs sont souvent tenus de créer des applications dans des délais très courts afin que l'équipe de virtualisation puisse les déployer et les gérer le plus rapidement possible. Par conséquent, l'équipe de sécurité n'est pas toujours au courant des changements qui interviennent dans l'environnement virtuel.

Vecteurs d'attaque critiques

Le centre de données et la mine d'informations qu'il abrite représentent la récompense ultime pour les cyberpirates. Toutefois, sauf si l'attaquant a la chance de trouver une vulnérabilité côté Internet, la compromission d'un centre de données exige du temps et de la préparation.

C'est pourquoi les cyberattaques contre les centres de données sont généralement des opérations mûrement réfléchies qui visent à s'assurer une présence durable au sein de l'environnement tout en échappant à la détection des équipes de sécurité.

Cette section s'intéresse aux vecteurs et techniques d'attaque critiques utilisés par les cyberpirates contre les centres de données.

Prise de contrôle de l'accès administrateur

Les administrateurs bénéficient du niveau d'accès le plus étendu au centre de données et sont à ce titre des cibles de choix pour les attaquants. Les protocoles d'administration permettent à ces derniers d'accéder au centre de données par une backdoor (porte dérobée) sans devoir directement exploiter une vulnérabilité présente dans une application. De plus, au moyen d'outils d'administration standard, comme SSH, Telnet ou RDP, les cyberpirates peuvent facilement faire en sorte que leurs activités se fondent dans le trafic d'administration normal.

Comme ces phases d'attaque utilisent des protocoles autorisés sans faire appel à des charges actives malveillantes, il est capital de recourir à des modèles d'analyse comportementale pour détecter les cybermenaces. Si possible, cette modélisation comportementale doit s'appliquer au trafic réseau réel car les journaux du protocole utilisé sont rarement disponibles.

L'authentification locale, une brèche à combler

Outre les pratiques standard utilisées par les administrateurs, de nombreux centres de données ont recours à des options d'authentification locale en cas d'urgence. Par exemple, en cas de défaillance d'un contrôleur de domaine ou d'une autre infrastructure d'authentification, l'administrateur doit pouvoir continuer à gérer le centre de données.

Dans de telles situations, il fait appel à l'authentification locale pour accéder aux systèmes et aux charges de travail à gérer. Toutefois, ces options d'authentification locale ne font pas l'objet d'une journalisation et les mêmes identifiants de connexion sont souvent partagés entre différents systèmes et charges de travail par souci de simplicité.

Bien qu'essentielles, ces méthodes mettent en péril la sécurité du centre de données. Lorsque les cyberpirates s'emparent des identifiants d'un administrateur, ils peuvent accéder au centre de données en toute impunité, sans crainte de voir leurs faits et gestes consignés dans les journaux.

La porte dérobée d'administration qui mène au matériel

L'authentification locale est un bel exemple de backdoor que les administrateurs – mais aussi les cyberpirates – peuvent employer pour accéder au centre de données. Il existe toutefois d'autres méthodes similaires qui vont plus loin, jusqu'au matériel sous-jacent.

Si virtualisé que soit le centre de données, il n'en demeure que les ressources et les environnements virtualisés doivent s'exécuter sur du matériel. Les disques virtuels dépendent au final des disques physiques, lesquels tournent sur des serveurs, eux aussi physiques.

Les serveurs physiques possèdent leurs propres plans de gestion hors bande et en service réduit. Ces plans de gestion disposent de leurs propres protocoles de gestion, modules d'alimentation, processeurs et mémoire, qui permettent à l'administrateur de monter les disques et de réimager les serveurs, et ce, même lorsque le serveur principal est hors tension.

Ces actions sont souvent effectuées par l'intermédiaire de protocoles, tels qu'IPMI (Intelligent Platform Management Interface). Si de nombreux fabricants de matériel possèdent leurs propres versions du protocole IPMI, par exemple iDRAC pour Dell ou ILO (Integrated Lights-Out) pour HPE, toutes sont basées sur IPMI et effectuent les mêmes fonctions.

Indépendantes du plan de données du serveur, ces fonctions sont situées sous les couches de virtualisation, en-dessous de tous les systèmes d'exploitation, et même sous le BIOS de la carte mère.

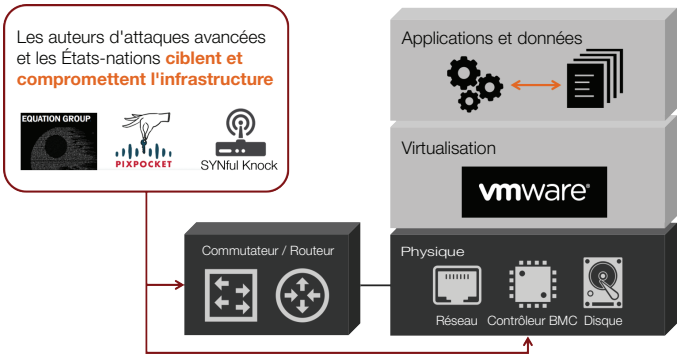
IPMI et les protocoles dérivés présentent des vulnérabilités de sécurité bien documentées et tardent souvent à recevoir les mises à jour et les correctifs. La combinaison des vulnérabilités d'IPMI et l'énorme potentiel qu'il offre font de ce protocole l'un des principaux maillons faibles de la sécurité du centre de données – ce qui n'échappe pas aux cyberpirates.

Les couches basses, cibles des attaques avancées

Malheureusement, les problèmes matériels du centre de données ne s'arrêtent pas au protocole IMPI. Les auteurs d'attaques avancées, dont les États-nations, ciblent de plus en plus souvent les serveurs physiques, les routeurs, les commutateurs et même les pare-feux.

Certains outils, comme SYNful Knock, ont démontré comment des cyberpirates peuvent se frayer un chemin sous le système d'exploitation pour prendre le contrôle administratif total d'un routeur et lancer par la suite des attaques contre d'autres systèmes et routeurs du même réseau.

Fondamentalement, ces outils sont des rootkits qui opèrent en-dessous du système d'exploitation, ce qui les rend extrêmement difficiles à détecter à l'aide des méthodes traditionnelles.



Les attaques du centre de données se concentrent sur l'infrastructure physique sous-jacente.

Les révélations à propos des outils d'attaque utilisés par le groupe Equation nous offrent un aperçu intéressant de l'arsenal et des techniques déployés par certains États. Ainsi, toute une série d'outils et de techniques sont employés pour implanter des logiciels et micrologiciels dans un large éventail de pare-feux et d'appliances de sécurité.

Ces techniques permettent d'infecter les équipements justement chargés de protéger le réseau et de les utiliser ensuite pour lancer des attaques s'infiltrant plus profondément au sein du réseau. Ici encore, la nature stratégique de ces dispositifs offre aux attaquants la possibilité de surveiller ou rediriger le trafic et de passer à l'offensive à partir d'un « poste de commande privilégié ».

Les données, l'objet de convoitise à surveiller de près

Le but ultime de la plupart des attaques est le vol des données. Par conséquent, la priorité absolue des équipes de sécurité doit être la détection des attaques bien avant qu'il n'y ait eu accès aux données, y compris lors de leur phase d'exfiltration.

Selon leurs besoins et compétences, les cyberpirates peuvent varier les techniques et méthodes utilisées pour faire sortir clandestinement les données du centre de données. La stratégie la plus logique consiste à exfiltrer les données en masse, en les transférant directement vers Internet ou vers une zone de transit dans le réseau de campus.

Les attaquants plus subtils peuvent adopter une approche « lente et furtive » en exfiltrant petit à petit les données, de façon à passer inaperçus et à ne pas éveiller les soupçons. Ils peuvent également chercher à occulter l'exfiltration des données, en les faisant passer par des tunnels dissimulés dans le trafic autorisé, par exemple le trafic web ou DNS.

L'association du contexte physique et virtuel

Les centres de données ont chacun leurs spécificités, qui varient selon l'entreprise à laquelle ils appartiennent, leurs applications et les interactions des utilisateurs avec celles-ci. À l'heure actuelle, le type le plus courant est le centre de données d'entreprise privé. Les attaques lancées à leur encontre sont généralement des extensions d'attaques menées contre l'environnement d'entreprise.

Ainsi, le cyberpirate peut avoir compromis au départ l'ordinateur portable d'un employé en recourant à un e-mail de phishing ou à l'ingénierie sociale. Ensuite, il va chercher à s'implanter durablement au sein du réseau en se déplaçant vers d'autres systèmes ou équipements.

Pour contrôler l'attaque en cours, le cyberpirate installe des backdoors ou des tunnels cachés dans le réseau pour empêcher la détection de son trafic de communication. Au fil du temps, il cartographie le réseau interne, identifie les ressources de valeur et, chemin faisant, compromet les équipements et les identifiants utilisateur.

Ce sont toutefois les identifiants administrateur que les cyberpirates convoitent le plus car ils lui garantissent une liberté quasi totale au sein du réseau infiltré. Ces identifiants jouent d'ailleurs un rôle essentiel dans les attaques des centres de données car les administrateurs sont bien souvent les seules personnes à pouvoir accéder aux données en masse.

Ce qu'il faut retenir, c'est qu'une attaque est généralement proche de son aboutissement lorsqu'elle atteint un centre de données privé. Le trafic C&C (Command & Control) dissimulé, la reconnaissance, le déplacement latéral et la compromission d'identifiants utilisateur et administrateur sont autant de conditions préalables à l'infiltration d'un centre de données.

Chacune de ces phases représente une occasion de détecter une attaque et il est capital que les équipes de sécurité jouissent d'une visibilité aussi complète que possible sur ce contexte avant que le centre de données ne soit touché.

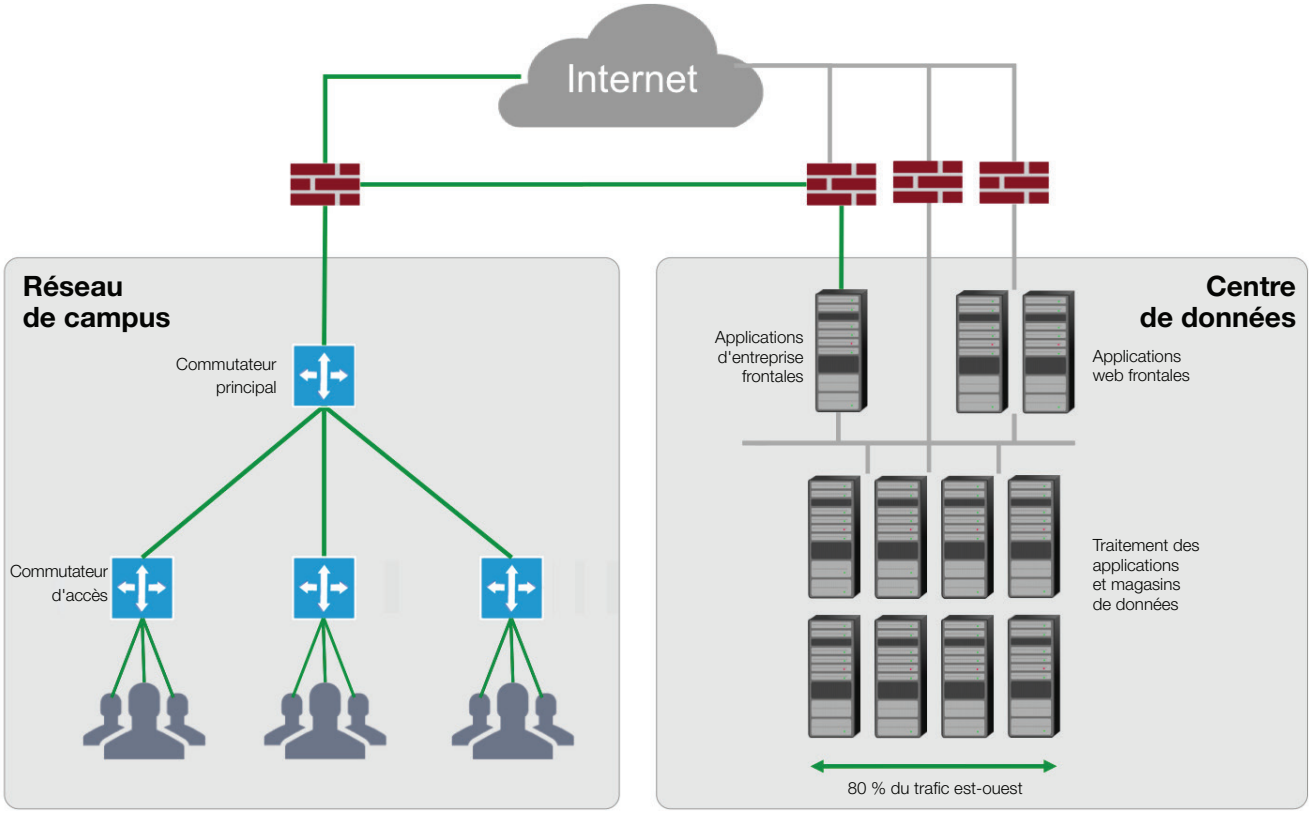
C'est pourquoi une approche globale et cohérente de la cybersécurité — du réseau de campus au centre de données en passant par les sites distants — est essentielle.

Les cyberattaques représentent des événements complexes et interconnectés. Dès lors, considérer la sécurité du centre de données comme une discipline isolée ne fait en définitive qu'aider les cyberpirates.

Conclusion

Compte tenu de l'abondance d'informations et d'applications qu'ils hébergent, les centres de données actuels représentent la mine d'or par excellence pour les cyberpirates. Or, malgré une sécurité essentiellement axée sur la protection de leurs couches virtualisées, les attaques qu'ils subissent visent de plus en plus à compromettre leur infrastructure physique.

Il est primordial de pouvoir identifier les cyberattaques qui ciblent les centres de données. Grâce aux modèles de détection avancée qui mettent au jour les attaques dirigées contre les couches applications, données et virtualisation du centre de données, ainsi que l'infrastructure physique sous-jacente, les équipes de sécurité seront en mesure de corriger les vulnérabilités critiques dans chaque couche du centre de données virtualisé.



La détection des cyberattaques exige une parfaite visibilité sur le réseau de campus et le centre de données.

VECTRA
Security that thinks®

E-mail : info_france@vectranetworks.com / info_dach@vectranetworks.com **Téléphone :** ++33 62 912 4119 / +41 44 551 0143
vectra.ai/fr