Fortinet et la santé

Soins de santé et ransomware : les prérequis d'une protection optimale

Les attaques via ransomware ont le vent en poupe. Avec l'essor du travail à distance et l'accès des collaborateurs aux réseaux par des moyens au niveau de sécurité aléatoire, la cybercriminalité a connu un pic au cours des derniers mois, les acteurs malveillants ayant profité de la migration soudaine vers le télétravail subie par nombre d'organisations. Les hackers opportunistes ont notamment identifié une cible particulièrement vulnérable sur laquelle se concentrer : les hôpitaux et les prestataires de soins de santé.

Dans toute l'Europe, les hôpitaux sont trop souvent les victimes d'attaques, entraînant la défaillance des systèmes informatiques et des conséquences parfois fatales.

De tous les secteurs à cibler, pourquoi celui des soins de santé en particulier ? Toutes les entreprises sont des cibles potentielles, mais les assaillants savent que les hôpitaux ne peuvent se permettre d'être à l'arrêt sur de longues périodes car des vies en dépendent. Leurs dirigeants seraient ainsi plus susceptibles de céder rapidement aux demandes de rançon pour assurer leur restauration post-ransomware, même si les autorités recommandent souvent le contraire. Et ce n'est pas la seule raison pour laquelle les hôpitaux sont des cibles particulièrement attrayantes.

Pourquoi les hôpitaux ?

L'élément principal qui fait des hôpitaux une cible aussi alléchante est la valeur des dossiers médicaux de patients sur le dark web. Les dossiers volés peuvent se revendre jusqu'à 1 000 $ pièce. Si l'on compare ce chiffre à celui des numéros de cartes de crédit, valorisés généralement à 5$, on comprend aisément pourquoi les cybercriminels ont les hôpitaux dans leur ligne de mire. Une fois qu'un ransomware a pénétré le réseau, il peut se propager et mettre hors service l'ensemble d'une infrastructure qui ne bénéficierait pas de mesures appropriées. Heureusement, il existe de nombreux moyens pour protéger les systèmes. Mais leur déploiement peut être complexe.

Malgré la diversité des outils disponibles pour juguler les ransomware, les hôpitaux, comme nombre d'entreprises, ont souvent du mal à déterminer où investir leurs budgets limités pour en tirer le meilleur bénéfice. Il est difficile de justifier le coût des mesures de sécurité lors de l'élaboration d'un budget IT, les systèmes de sécurité ne pouvant fournir des prévisions fiables en matière de retour sur investissement. Tenter de justifier le coût d'une perte de données, qui peut ou non se produire, peut s'avérer très compliqué, surtout lorsque les dirigeants, les politiciens et le grand public ne comprennent pas toujours les subtilités du contexte.

Aucun organisme, qu'il soit public ou privé, ne veut être vulnérable. Il s'agit de tirer le meilleur parti du budget dont il dispose et d'affecter les ressources financières, peu ou prou importantes, de manière pertinente. Quelles sont donc les mesures de sécurité à privilégier ?

Rester à l'abri

Même si les ransomware ne sont pas nécessairement plus sophistiqués que d'autres formes de logiciels malveillants, ils restent un moyen couramment utilisé par les pirates. En plus de veiller à ce que les sauvegardes de données soient effectuées en temps voulu, de manière complète et sécurisées hors site, les hôpitaux doivent envisager une stratégie de sécurité à plusieurs niveaux, comprenant des technologies de prévention, de détection et de réponse aux incidents, déployées de manière appropriée sur tous les points d'entrée possibles au réseau.

Les technologies réseau telles que la prévention des intrusions (IPS) et les antivirus (AV) ne sont que quelques-unes des solutions de prévention à envisager. D'autres options spécifiques sont disponibles, comme une passerelle de sécurité email (la messagerie restant l'un des points d'entrée les plus courants) et la protection des applications Web à l'aide d'un pare-feu d'application Web (WAF). Une fois qu'une couche de prévention efficace est en place, il est possible de déployer des technologies clé de type EDR (Endpoint Detection & Response) ou sandbox. D'autre part, pour s'assurer que seuls les utilisateurs et dispositifs autorisés peuvent se connecter au réseau, le contrôle d'accès au réseau (NAC) est un complément idéal pour surveiller les travailleurs à distance. Il est également important d'évaluer l'intérêt d'une solution SIEM offrant une analyse en direct des menaces sur la base de données provenant de l'ensemble de l'architecture informatique. Alternativement, le choix peut porter sur une technologie XDR, qui collecte des données provenant de toutes les couches de sécurité et les corrèle, afin d'éviter qu'une menace identifiée sur un domaine ne se propage pas vers d'autres.

Une approche multicouche permet de minimiser la pénétration des malware sur le réseau et empêche également ceux qui ont réussi à s'immiscer de se propager.

Cependant, même avec la meilleure protection du monde, il est important de rappeler qu'environ 99% des attaques impliquent une erreur humaine pour accéder au réseau d'un hôpital. Les pirates comptent sur le fait que les utilisateurs cliquent sur un lien, téléchargent un fichier malveillant ou divulguent par inadvertance des informations telles que des mots de passe. Se former à la "cyber-hygiène" est donc devenu aussi crucial que l'hygiène médicale. Avec un personnel sensibilisé aux bonnes pratiques et capable d'y réfléchir à deux fois, une entreprise est déjà sur les rails d'une sécurité robuste.

Perspectives autour de la sécurité

Alors que la digitalisation des soins de santé se poursuit grâce à des services tels que la télémédecine ou la consultation par vidéo, ce secteur est plus productif et plus accessible que jamais. Mais cela signifie aussi que la sécurisation du réseau sous-jacent et de tous les systèmes et dispositifs connectés est plus importante que jamais. Les hôpitaux doivent rechercher des approches de cybersécurité automatisées, intégrées et globales auprès de fournisseurs qui comprennent les spécificités de ce secteur, d'autant plus que la 5G et l'IoT continuent de gagner en popularité.

La mise en place de ces mesures de protection ne doit pas nécessairement siphonner la majeure partie du budget d'un hôpital, ni nécessiter des connaissances techniques approfondies. Elle requiert néanmoins un support interne adéquat et un état d'esprit proactif. Après tout, comme le savent tous les professionnels de santé, il est toujours plus pertinent de prévenir que de guérir.