SÃ©curitÃ© du e-commerce B2B : risques, mesures et solutions
SÃ©curitÃ©
PostÃ© par : JerryG
PubliÃ©e le : 27/9/2023 13:00:00

Les cybercriminels disposent de plusieurs faÃ§ons d'exploiter les vulnÃ©rabilitÃ©s du SI pour accÃ©der aux donnÃ©es de l'entreprise. Les vecteurs d'attaque peuvent inclure tout, depuis les virus, les logiciels malveillants, les piÃ¨ces jointes, les sites Web et les actes d'ingÃ©nierie sociale.

Cependant, une cybermenace se distingue des autres comme la plus sophistiquÃ©e et la plus dÃ©sastreuse : le ranÃ§ongiciel. Les attaques par Ransomware constituent une menace constante pour les entreprises B2B, en particulier avec la montÃ©e en puissance du e-commerce B2B. Heureusement, avec les bons outils et la bonne stratÃ©gie, il est possible de se protÃ©ger de ces menaces.

Qu'est-ce que la sÃ©curitÃ© du e-commerce B2B ?

La sÃ©curitÃ© dans le e-commerce B2B fait rÃ©fÃ©rence aux mesures et protocoles mis en place pour protÃ©ger les transactions en ligne et les informations sensibles des clients, tels que les dÃ©tails de la carte de crÃ©dit ou les identifiants de connexion. Cela implique de protÃ©ger l'intÃ©gritÃ©, la confidentialitÃ© et la disponibilitÃ© des donnÃ©es, ainsi que d'empÃªcher l'accÃ¨s non autorisÃ©, la fraude et les cybermenaces.

Les mesures de sÃ©curitÃ© du e-commerce B2B comprennent la mise en Å□uvre de passerelles de paiement sÃ©curisÃ©es, de technologies de cryptage, de pare-feu et de processus d'authentification robustes pour garantir que les donnÃ©es des clients et les transactions financiÃ¨res sont traitÃ©es en toute sÃ©curitÃ©. En priorisant la sÃ©curitÃ© du e-commerce, les entreprises peuvent Ã©tablir une relation de confiance avec leurs clients et protÃ©ger leurs informations sensibles contre les menaces potentielles.

Pourquoi le Ransomware est-il un problÃ¨me dans le e-commerce B2B ?

De nombreuses entreprises B2B sont entrÃ©es depuis peu dans l'arÃ¨ne du e-commerce et ont Ã©tÃ© contraintes d'adopter de nouvelles mÃ©thodes de vente et de nouvelles faÃ§ons de rÃ©pondre aux attentes des clients.

Des acteurs malveillants tirent avantage de ce manque de maturitÃ© pour accÃ©der aux donnÃ©es et aux processus essentiels de ces acteurs du B2B. De l'exploitation des vulnÃ©rabilitÃ©s non corrigÃ©es Ã l'ingÃ©nierie sociale, aux attaques DDOS, aux logiciels malveillants et aux virus, il existe de nombreuses faÃ§ons de compromettre les systÃ¨mes d'entreprise.

Les ransomwares privent les entreprises B2B des donnÃ©es et des systÃ¨mes dont elles ont besoin pour exÃ©cuter des fonctions critiques. A mesure que la fraude et les attaques se dÃ©veloppent, lâ□□impact financier des ranÃ§ongiciels augmente.

Quelles entreprises e-commerce B2B sont Ã risque ?

A l'origine, les cyberattaques visaient des systÃ¨mes informatiques uniques ou des utilisateurs individuels. Au fil du temps, les cybercriminels ont rÃ©alisÃ© qu'il y avait plus de potentiel Ã cibler les entreprises.

Aujourd'hui, les attaquants ciblent les industries et les groupes qui, selon eux, leur apporteront un plus grand pouvoir de nÃ©gociation et des chances plus Ã©levÃ©es de payer des ranÃ§ons importantes. Les organisations ciblÃ©es sont notamment les entreprises dans les pays occidentaux, les grandes entreprises ou encore les petites et moyennes entreprises.

Menaces de sÃ©curitÃ© pour le e-commerce

Il existe des moyens pratiquement illimitÃ©s d'exposer, de modifier, de dÃ©sactiver ou dâ□□impacter un SI. Pour les vendeurs en ligne en particulier, tout, pas seulement les systÃ¨mes informatiques physiques, mais aussi les logiciels, les rÃ©seaux et l'infrastructure, sont exposÃ©s aux failles de sÃ©curitÃ©.

Ces entreprises ont besoin de disponibilitÃ© et prÃ©fÃ¨rent payer la ranÃ§on plutÃ´t que dâ□□Ãªtre paralysÃ©es. Une seule panne peut crÃ©er des interruptions et des pÃ©nuries de la chaÃ®ne d'approvisionnement, une perturbation des services essentiels et des rÃ©percussions pour le consommateur.

Pour ceux qui travaillent sur le segment B2B, il nâ□□est pas possible de nÃ©gliger les aspects de sÃ©curitÃ© du e-commerce, aussi mineurs soient-ils. Contrairement aux vendeurs B2C, les vendeurs B2B traitent des produits plus complexes, une clientÃ¨le plus diversifiÃ©e et gÃ¨rent des volumes de commandes plus importants. Les valeurs Ã©levÃ©es des commandes et la fidÃ©litÃ© des clients attirent Ã©galement l'attention des cybercriminels.

Positionner la cybersÃ©curitÃ© au centre de son projet e-commerce B2B est donc un prÃ©requis pour tisser avec ses clients une relation de confiance. Par ailleurs, câ□□est Ã©galement une nÃ©cessitÃ© pour ne pas voir son organisation impactÃ©e et bloquÃ©e par des cyberattaquants, dixit Laurent Desprez chez ORO.inc