Ransomware

enuve

Ramsonware, o sequestro de dados que está vitimando as empresas

Quais os impactos para o seu negócio ?

Imagine que é um dia típico. Você acorda, chega no escritório, serve uma xícara de café e liga seu computador para iniciar mais um dia de trabalho. Porém algo está diferente desta vez. Em vez de o computador inicializar sem problemas e exibir a área de trabalho, você é recebido com uma janela assustadora, com a imagem de um cadeado. O texto nessa janela informa que seus dados foram bloqueados e ficarão permanentemente inacessíveis após alguns dias, a menos que um resgate seja pago. O valor e o método de pagamento podem variar, mas a ameaça não: Pague ou nunca mais veja seus dados. Surpresa. Você acabou de se tornar a vítima mais recente de um ataque de ransomware.

Mas o que é exatamente um Ransomware ?

Conhecido como o vírus de resgate, o Ransomware vem sendo utilizado por hackers para o sequestro de dados. Desde 2015 tem crescido exponencialmente. Após ser executado, com ou sem a autorização do usuário, ele trata de codificar todos os dados do computador em questão. Para acessá-los novamente, é necessária uma senha, que está em posse do indivíduo que controla o ransomware. Essa pessoa, então, cobra um valor para liberar os arquivos do dispositivo afetado

enuve

E quais os **impactos** para sua empresa?

Impede o acesso aos seus dados

O ransomware é uma ameaça significativa para os seus negócios, porque criptografa seus dados, o que impede que você os acesse. A única maneira de desbloquear os dados é usando uma chave de descriptografia que apenas o hacker controla. Na maioria das vezes, essa chave será fornecida à organização após o pagamento do resgate. No entanto, em alguns casos, os dados nunca são liberados. As vítimas de ransomware são de todas as formas e tamanhos. Alguns empresários acreditam que nunca serão vitimados porque a empresa é muito pequena. Isso não é verdade. Uma grande proporção de ataques de ransomware ocorre quando uma pequena vulnerabilidade de segurança é aproveitada pelos hackers.

Interrompe operações

Por si só, o ransomware não é o risco mais significativo. O risco real ocorre com o impacto operacional que o ransomware pode ter nos negócios. Tente visualizar um processo ou serviço vital da sua empresa que imediatamente para. O Ransomware tem a capacidade de encerrar divisões ou toda a planta, congelar sistemas de controle de fabricação, atingir a câmara e compensação de um banco ou causar outros atrasos. As perdas devido ao tempo de inatividade podem ser significativas e ter consequências consideráveis.

enuve

Danos à reputação

Muitas vezes, um ataque cibernético a uma organização se torna público. Tornar-se vítima de ransomware pode afetar a confiança entre você e seus consumidores. Simplificando, os consumidores não confiarão mais na empresa. Os clientes podem se sentir inseguros para enviar online suas informações pessoais ou de cartão de crédito.

Custos financeiros

Uma estratégia disciplinada de backup e recuperação não tornará necessariamente um ataque de ransomware livre de problemas, pois pode levar uma quantidade considerável de tempo e dinheiro para restaurar os dados. A decisão de recuperar seu sistema usando um backup dependerá da quantidade de perda de dados considerada aceitável para a sua organização, da extensão em que ela se espalhou e da rapidez com que o comprometimento foi detectado. No entanto, algumas vezes os dados ficam tão criptografados que você pode não ter permissão para retornar a um ponto de restauração anterior. Por isso, uma boa alternativa são os backups em nuvem.

Conclusão

Independentemente do tamanho da sua empresa, você pode se tornar vítima de ransomware. Se ocorrer uma violação, poderá custar tempo de inatividade, uma perda financeira imediata e significativa e danificar permanentemente sua reputação. Portanto, é essencial implantar uma estratégia para proteger seus ativos contra hackers.

enuve