Checklist Eaton de melhores práticas de segurança

26 de Fevereiro, 2019

A Eaton, empresa de gestão energética, concebeu uma lista de boas práticas para fazer frente à ciberatividade maliciosa e aos perigos presentes online. Numa altura em que os hackers estão particularmente ativos e que a preocupação com atividades dolosas na maior das redes está a aumentar, as empresas devem proteger-se com políticas de segurança responsáveis e bem implementadas, compreendendo os imperativos de salvaguarda de dados e de garantia de continuidade do negócio subjacentes a estas políticas.

A Eaton recomenda assim:

Cópias de segurança: a empresa deve colocar a si mesma a questão dos backups – as cópias de segurança incluem toda a informação crítica da empresa? Estão guardadas offline? É possível repor os dados em caso de necessidade? A Eaton recomenda uma política de backups baseada em cópias totais semanais e backups incrementais diários para garantir a salvaguarda dos dados.

Análise de risco: foi elaborado algum tipo de análise de riscos de cibersegurança na organização? A Eaton colabora amiúde com empresas de segurança para levar a cabo auditorias de sistemas. A empresa tem as competências necessárias para aconselhar as empresas quanto às políticas de análise de riscos.

Formação é palavra de ordem: ter uma força de trabalho preparada para lidar com os riscos de cibersegurança é a primeira linha de defesa da empresa. A Eaton conta com um programa denominado "Helping Utilities Meet NERC CIP" que ajuda a implementar ou melhorar os programas de formação do staff mesmo em cenários onde não há necessidade de conformidade com NERC CIP. Esta formação e as medidas presentes nas políticas de segurança são essenciais para limitar o espetro dos ataques.

Monitorização de vulnerabilidades e patching: as empresas devem ter em consideração a premente necessidade de implementar patches abrangentes e processos de atualização dos servidores e dos PCs dos colaboradores.

Whitelisting: as aplicações que são executadas na rede da empresa estão numa whitelist? A Eaton publica requisitos mínimos de sistema a cada publicação do Yukon. Todas as aplicações não necessárias são removidas das listas presentes nos servidores facultados aos clientes. Além disso, recomenda-se que estes desliguem todas as portas não utilizadas nas firewalls.

Continuidade de negócio: a empresa deve estar preparada para assegurar a continuidade do negócio mesmo sem acesso a determinados sistemas. Neste aspeto em particular, os eventos de segurança como os que estão relacionados com os mais recentes ataques de ransomware devem ser encarados como oportunidades para as empresas testarem, reverem e se possível exercitarem os

seus planos de continuidade.

Testes de permeabilidade: conheça bem os seus sistemas. Os responsáveis da empresa devem eles mesmo tentar entrar nos sistemas para testar as proteções e as capacidades de defesa. A Eaton tem um longo histórico de testes de vulnerabilidade às suas smart grids e pode facultar linhas de ação a empresas que queriam fazer os seus próprios testes.

Filipa Soares, responsável de Marketing da Eaton, explica que “a equipa de smart grid da Eaton e o seu Cybersecurity Center of Excellence (CCoE) fizeram uma cuidada análise aos mais recentes ciberataques e acreditam que estes eventos facultam uma oportunidade de reforçar junto dos clientes a importância de assegurar o cumprimento da lista de boas práticas no campo da cibersegurança”. A mesma responsável sublinha a relevância desta lista e salienta a necessidade das empresas não facilitarem neste cenário em particular, algo que teria consequências dolosas para a empresa e para a continuidade do negócio.