CRÓNICA VISÃO ELECTRÓNICA
Nº 525 / 2019-02-07
http://www.gestaodefraude.eu
Edgar Pimenta

>> *Shutdown* à Segurança

É o *shutdown* mais longo dos Estados Unidos.

Por falta de acordo para a construção de um muro que separe o México dos Estados Unidos, estes últimos entraram em *shutdown*. Basicamente o que *shutdown* faz é fechar o financiamento de diversas agências e operações governamentais americanas, fazendo com que estas agências e operações operem com níveis mínimos de serviço. Assim, tudo o que não seja serviço essencial poderá fechar.

E o que tem isto a ver com Segurança?

A segurança de informação (pois é nesse âmbito que usamos aqui a palavra segurança) é um processo. Um processo que inclui diversas vertentes e sub-processos que devem funcionar em perfeita articulação para proteger de forma efetiva a informação das empresas.

Um dos sub-processos é a gestão de vulnerabilidades.

Embora os sistemas devam ser construídos de uma forma que assegurem a sua segurança, a verdade é que não existem sistemas perfeitos. Seja durante o processo de criação de sistemas seja durante a sua manutenção, podem existir problemas que podem afetar segurança dos sistemas (vulnerabilidades). Essas vulnerabilidades podem ser eventualmente exploradas para comprometer os sistemas.

Assim, um processo de gestão de vulnerabilidades consiste em identificar quais as vulnerabilidades que os sistemas apresentam para que possam depois ser mitigadas.

Obviamente, seguindo um princípio de gestão de risco, aquelas vulnerabilidades mais críticas e/ou que afetam os sistemas mais importantes devem ser mitigadas rapidamente.

Enquanto um sistema apresenta vulnerabilidades e estas não são resolvidas ou compensadas com outros controlos, existem riscos para os sistemas das empresas.

Outro sub-processo associado à segurança e provavelmente um dos mais conhecidos de todos, é a gestão de acessos. Os seus objetivos são simples: i) garantir que quem precisa de um acesso o têm, seguindo um processo definido com aprovação e devidamente adequado à função; ii) garantir que enquanto um utilizador está na empresa, os seus acessos estão adequados às funções e, finalmente, iii) garantir que o acesso é cancelado quando a pessoa deixa de precisar do mesmo (ex: saída).

É um lugar-comum dizer que os utilizadores são o elo mais fraco da segurança. Mas a verdade é que muitas vezes esse lugar-comum corresponde à realidade. Por isso, o processo acima apresenta uma criticidade maior.

Estes processos acima indicados (e outros que poderiam ser enumerados) não são normalmente considerados como essenciais para a operação de uma empresa. E em situações como o *shutdown* nos Estados Unidos, pode levar à sua não realização, com impactos na segurança que podem críticos.

Sem dúvida que o modo como é vista a segurança da informação mudou muito nos últimos anos. Deixou de ser um tema algo esotérico para ser um tema verdadeiramente na ordem do dia. E para isso, não podemos esquecer o papel que regulação e legislação tem tido, sendo o RGPD (Regulamento Geral de Proteção de Dados) sem dúvida um alavancador de muitas iniciativas de segurança.

Mas falta o passo seguinte. Falta passarmos a ver a segurança da informação como algo basilar para o funcionamento de uma organização, a par de outras funções. E a segurança da informação ser essencial.