Debate – Agenda 06

Tecnologia da Informação III

Mônica Zungalo Quintal

"Com o grande e rápido avanço que a tecnologia digital teve nas últimas duas décadas, continuamente problemas de segurança são descobertos e as suas soluções, ou tentativa delas, são publicadas pelos fabricantes de software e hardware. Um grande exemplo disso é que o Microsoft Windows possui um ciclo de atualizações mensais de segurança, ou se o problema for muito grave, assim que a correção (patch) é terminada ela é disponibilizada por meio do Windows Update.

Debata com os colegas e com o Professor-Mediador sobre como um Técnico da área de Tecnologia da Informação deve proceder para implementar um patch de segurança em uma rede de uma empresa com um grande número de computadores de modo eficiente."

A palavra Patch, traduzindo do inglês, significa “correção”. Ou seja, patch de segurança consiste em uma atualização de software projetada para corrigir vulnerabilidades ou falhas de segurança, seja em um programa, sistema operacional ou dispositivo. Ou seja, são importantes para manter sistemas e redes seguros, considerando que essas vulnerabilidades podem ser exploradas por hackers ou malwares, comprometendo a segurança, além de roubar informações e/ou causar danos. Os patches de segurança geralmente são lançados pelos fornecedores de software após a descoberta de uma vulnerabilidade.

Antes de implementar um patch, é importante avaliar possíveis vulnerabilidades na rede. Posteriormente, o Técnico de TI deve priorizar os patches de acordo com a sua gravidade e importância para o ambiente, lembrando que, antes de implantar patches em produção, deve-se testá-los, para que não ocorram problemas de compatibilidade ou de desempenho. Também é necessário planejar o momento e a logística da implantação, minimizando o impacto nas operações da empresa.

Conforme estudado nesta agenda, é muito importante que a empresa possua backup de seus arquivos, e neste caso, principalmente dos sistemas, antes que sejam aplicados os patches. Isso garante que, se algo der errado, seja possível restaurar os sistemas para um estado funcional. Também é imprescindível que o Técnico monitore a implantação de patches, e que mantenha registros detalhados, além de monitorar as vulnerabilidades de forma contínua.