

Trabalhando com servidores proxy e firewalls em nível de aplicativo*

Ron Hall estava sonhando com suas próximas férias. Ele trabalhava para Andy Ying, gerente do grupo de consultoria de segurança, em um projeto muito exigente, há quase seis meses.

Hoje ele finalmente terminou o trabalho e teve alguns minutos para navegar na Web e planejar sua próxima viagem à Nova Zelândia.

Ron sabia que a ATI não permitia a navegação indiscriminada na Web e que eles usavam um servidor proxy para garantir a conformidade com essa política, mas ele sentiu que merecia esse tratamento e acreditava que Andy não teria problemas com um pouco de navegação recreativa na Web. Além disso, eram quase 17h e estava quase na hora de ir para casa.

O Google foi autorizado pelo servidor proxy, então Ron foi até lá para iniciar sua busca. Ele digitou “pontos de férias na Nova Zelândia”. Mais rápido do que ele conseguia piscar, o gigante mecanismo de busca Google voltou com uma lista de links relevantes. A primeira entrada parecia promissora: “New Zealand Tourism Online: New Zealand Travel Guide”. Mas o segundo ficou ainda melhor: “Fotos da Nova Zelândia”. Ele clicou nesse URL.

Nenhuma imagem foi aberta. Nada de vales verdes. Sem recifes de coral. Nada de belas montanhas. Apenas uma tela branca com letras pretas que diziam:

ACESSO PROIBIDO — ENTRE EM CONTATO COM O ADMINISTRADOR DO PROXY SERVER PARA INSTRUÇÕES DE COMO ACESSAR O CONTEÚDO SOLICITADO.

Ron não ficou surpreso, mas esperava. Ele clicou no botão “Voltar” e tentou o próximo link. Ele recebeu a mesma mensagem. Ele tentou mais três ou quatro vezes e então percebeu que não estava conseguindo nenhuma foto hoje.

Ron chegou à sua mesa um pouco cedo na manhã seguinte. Ele ligou seu PC e foi tomar uma xícara de café enquanto ele inicializava. Quando voltou, abriu seu programa de e-mail. Na lista de novos e-mails havia uma nota do grupo de segurança de rede. Ele abriu a mensagem e viu que tinha sido endereçada a ele e a Andy Ying, seu chefe. Também tinha um CC para o departamento de RH. A mensagem dizia:

Recentemente, sua conta foi usada para acessar conteúdo da Web que não foi aprovado para uso dentro da ATI. Estamos pedindo que você explique suas ações ao seu supervisor. Você é encorajado a se matricular em um curso sobre uso apropriado da Internet na ATI o quanto antes. Até que você complete a aula ou seu supervisor entre em contato com este escritório, seus privilégios de rede foram suspensos. Se esta tentativa de acesso foi para fins comerciais legítimos, peça ao seu supervisor que nos notifique imediatamente para que este local da Web possa ser adicionado à lista de locais da Web aprovados pela ATI.

Que aborrecimento. Ron não estava ansioso por sua conversa com Andy.

Questões

1. A política da ATI sobre o uso da Web parece dura para você? Por que ou por que não?

Resposta do grupo:

sim, pois a rede da empresa precisa ser protegida de sites desconhecido.

Comentários do professor:

A política era rigorosa, mas, como consultor de segurança, “Ron sabia que a ATI não permitia a navegação indiscriminada na Web e que eles usavam um servidor proxy para garantir a conformidade com essa política”. Acreditou que poderia ter tratamento diferenciado por ser da equipe de segurança. Normalmente, políticas de segurança devem ser aplicadas a todos.

Sobre a resposta do grupo: “a rede da empresa precisa ser protegida de sites desconhecido”, o problema não é o site ser desconhecido, mas não estar de acordo com o propósito da empresa.

2. Você acha que Ron foi justificado em suas ações?

R: Sim, a política pode parecer rígida, mas ela é necessária para garantir a segurança da rede corporativa. A empresa utiliza um servidor proxy para monitorar e controlar o acesso à web, o que ajuda a proteger contra sites que não são relevantes para os negócios e possíveis riscos de segurança. Embora a política possa parecer rígida, ela é importante para garantir que todos sigam as mesmas diretrizes e não haja exceções, mesmo para membros da equipe de segurança. Como consultor de segurança, Ron sabia que a navegação indiscriminada não era permitida e deveria respeitar as normas da empresa, independentemente de sua função.

3. Como Andy deve reagir a essa situação se Ron é conhecido por ser um funcionário confiável e diligente?

R: Não, Ron não foi justificado. Apesar de ser parte da equipe de segurança, ele sabia das restrições de navegação e da política de controle de acesso à web implementada pela ATI. Ele foi claramente avisado pela mensagem de "acesso proibido" que apareceu várias vezes, mas insistiu em tentar acessar conteúdos que não estavam aprovados. Embora ele possa ter acreditado que, por ser da equipe de segurança, teria tratamento diferenciado, as políticas de segurança devem ser aplicadas de forma uniforme a todos os funcionários, independentemente de sua posição. Por isso, as ações de Ron não foram justificadas.

*WHITMAN, Michael E. MATTORD, Herbert J. **Readings and Cases in Information Security: Law and Ethics.** Course Technology, Cengage Learning: Boston (MA), 2011.