Por **Alexandre Sammogini**

E mantenha a “guarda fechada” no ringue, pois as ameaças continuam !!!. Desta vez, a vítima foi a Lojas Renner S.A., maior varejista de moda do Brasil em faturamento. Um ataque de hacker, ocorrido numa quinta-feira, 19 de agosto de 2021, deixou seu site sem funcionar até o sábado seguinte, ao passo que o seu aplicativo de compras somente foi restabelecido no domingo. De acordo com a empresa, não houve contato com os autores desse ataque e nem negociação de pagamento de resgate de qualquer espécie.

E os casos não param por aí, já que os ataques cibernéticos cresceram significativamente durante a pandemia da Covid-19, no mundo todo. Nesse cenário tão complexo e inseguro, a grande preocupação para as organizações, de um modo geral, é assegurar que ao fornecer aos seus usuários acesso aos sistemas e dados institucionais, o seu ambiente digital permaneça seguro. Por isso, não devemos nunca nos esquecer de que qualquer usuário que tenha acesso a rede da organização e não tome as devidas precauções compromete a segurança corporativa.

E nada mais apropriado, portanto, do que tratarmos nesta edição da porta de entrada e saída das informações e dados de uma empresa, descrevendo a importância do Processo de Gestão de Contas e Usuários.

Nesse sentido, as entidades devem realizar o controle de contas e usuários para proteger suas informações e os cuidados devem envolver tanto usuários internos quanto externos. O gerenciamento consiste em realizar o controle dos ativos e dos recursos digitais corporativos, ou seja, verificar os privilégios dos colaboradores, assim como as permissões de acesso aos recursos tecnológicos e sistemas da empresa, permitindo que cada colaborador tenha acesso apenas ao necessário para executar sua função. Isso abrange os dispositivos, aplicativos, sistemas de armazenamento, redes e outros.

Por meio do gerenciamento de contas e usuários, a área de TI alcança um alto nível de controle sobre seus dados e sistemas, garante eficiência para que as atividades não sejam interrompidas e minimiza as vulnerabilidades ou brechas de segurança. Para isso, é necessário realizar o controle de acesso, processo este realizado em três etapas, sendo todas de suma importância para a perfeita implantação e gestão de contas e usuários. Cada etapa reforça um ponto importante a ser observado na gestão de segurança da informação, entre os quais podemos destacar:

- a autenticação determina a permissão e os acessos cedidos a cada usuário da entidade;
- a autorização elenca o que cada usuário tem permissão para acessar e realizar no sistema, ou seja, determina os níveis de permissão e os delimita de acordo com a sua função na entidade, devendo ser imediatamente revogada em caso de desligamento do colaborador dessa; e
- a auditoria visa verificar se o colaborador utilizou da sua permissão de forma adequada ou mal intencionada e, por isso, o sistema realiza a coleta dos históricos de uso dos recursos tecnológicos de cada usuário (esses dados são utilizados para possíveis verificações futuras caso algum erro aconteça).

É indispensável ao controle de contas e usuários investir em uma ferramenta que possa garantir a segurança e eficiência de seus sistemas, além de fornecer acesso adequado a todos os usuários. Entre outros benefícios, ainda podemos destacar a redução da complexidade dos acessos, a hierarquização das permissões, a automação e a centralização da gestão.

A seguir, apresentamos um quadro resumo de sugestões de pontos que devem ser observados na gestão de contas e usuários.

1. Proteger contas dedicadas de auditoria	Utilização de contas dedicadas para análises de vulnerabilidades autenticadas, que devem ser segregadas de

	contas de demais atividades administrativas e devem estar vinculadas a máquinas específicas em endereços IP específicos.
2. Atualizar o inventário de contas administrativas	Emprego de ferramentas automatizadas para inventariar todas as contas administrativas, incluindo contas locais e de domínio, para garantir que apenas indivíduos autorizados tenham privilégios elevados.
3. Alterar senhas padrão	Alteração de todas as senhas padrão antes de qualquer implantação de novo ativo, para que as mesmas estejam sempre consistentes com o nível de senhas das contas de nível administrativo.
4. Utilizar estações de trabalho dedicadas para todas as tarefas administrativas	Garantia de que os administradores utilizem uma máquina dedicada para todas as tarefas administrativas ou tarefas que requerem acesso administrativo. Máquina esta segmentada da rede principal da organização e que não possua acesso à Internet. Esta máquina não pode ser usada para ler e-mails, redigir documentos ou navegar na Internet.
5. Utilizar senhas exclusivas	Onde a autenticação Multifator não é suportada (como administrador local, raiz ou contas de serviço), as contas utilizam senhas exclusivas para estes sistemas.
6. Utilizar a autenticação Multifator (1) – MFA – para todo acesso administrativo	Utilização de autenticação com MFA e canais criptografados para todo o acesso a contas administrativas.
7. Assegurar o uso de contas administrativas dedicadas	Garantia de que todos os usuários com conta de acesso administrativo utilizam uma conta dedicada ou secundária para atividades de privilégios elevados. Essas contas devem ser usadas apenas para atividades administrativas e não para navegação na Internet, e-mail ou atividades similares.
8. Limitar o acesso a ferramentas de script	Limitação de acesso a ferramentas de script (como Microsoft® PowerShell e Python) apenas para usuários administrativos ou de desenvolvimento com a necessidade de acessar esses recursos.
9. Gerar logs e alertas em casos de logon malsucedido em contas administrativas, assim como sobre as alterações em membros do grupo administrativo	Configuração de sistemas a fim de emitir uma entrada de log e alertar quando uma conta é adicionada ou removida de qualquer grupo com privilégios administrativos.
10. Exigir que todo o logon remoto use autenticação de múltiplos fatores	Obrigatoriedade de, em todo acesso remoto à rede da organização, a criptografia de dados em trânsito e o controle de acesso utilizar autenticação Multifator (MFA).
11. Manter inventário de sistemas de autenticação	Manutenção de inventário de cada um dos sistemas de autenticação da organização, incluindo aqueles sistemas on premise (2) ou hosteados (3) em um provedor de serviços remoto.
12. Configurar um ponto central de autenticação	Configuração do acesso a todas as contas através do menor número possível de pontos centralizados de autenticação, incluindo sistemas de rede, segurança e nuvem.
13. Requerer autenticação MultiFator	Exigência de autenticação Multifator para todas as contas de usuário, em todos os sistemas, e que sejam eles gerenciados on premise ou por um provedor de terceiros.
14. Criptografar ou cifrar todas as credenciais de autenticação	Criptografia ou geração de todas as credenciais de autenticação para o armazenamento.
15. Criptografar a transmissão de nome de usuário e credenciais de autenticação	Verificação se todos os nomes de usuário e credenciais de autenticação de contas de usuários são transmitidos pelas redes, utilizando canais criptografados.
16. Manter atualizado o inventário de contas	Manutenção de inventário de todas as contas organizadas pelo sistema de autenticação da organização.

17. Estabelecer processos para revogação de acessos	Estabelecimento de processo automatizado para revogação de acessos sistêmicos, desativando as contas imediatamente após o término ou alteração das responsabilidades dos usuários (desabilitando essas contas, em vez de realizar a sua exclusão, permitindo a preservação de trilhas de auditoria).
18. Desativar contas não associadas	Desativação de qualquer conta que não possa ser associada a um processo corporativo ou a um proprietário delegado da organização.
19. Desativar contas inativas	Desativação, automaticamente, de contas inativas dormentes após um período definido de inatividade.
20. Garantir que todas as contas tenham uma data de expiração	Certificação de que todas as contas tenham uma data de validade monitorada e aplicada.
21. Travar sessões em estações de trabalho após período de inatividade	Bloqueio automático das sessões das estações de trabalho após um período padrão de inatividade.
22. Monitorar tentativas de acesso a contas desativadas	Monitoria de tentativas de acesso a contas desativadas através de logs de auditoria.
23. Alertar sobre desvios de comportamento de login em contas	Controle com alerta de quando os usuários se desviam do comportamento normal de login, como hora do dia, local da estação de trabalho e duração do acesso.

That’s all folks! Continue atento e não perca a nossa próxima edição: – “Saiba como tornar seus processos de T.I. robustos e capazes de prevenir ataques cibernéticos – Parte III”.

***Comissão Técnica Regional Leste de Governança e Riscos – Parte II**

Notas:

1. Do inglês Multifactor Authentication, consiste em uma ação que confirma a autenticidade do usuário que efetua a requisição de um determinado serviço na web.
2. O servidor on premise tem sua implantação fixada no local da empresa e requer um planejamento mais detalhado.
3. Ação de hospedar ou manter um site em uma rede.

Fonte: Abrapp em Foco, em 23.09.2021.