Mantenha o seu negócio seguro mesmo quando for necessário o trabalho remoto

O Diretor de Segurança da Informação da Alcatel-Lucent Enterprise, Sebastien Roche, compartilha insights sobre a abordagem da ALE em relação à continuidade e segurança dos negócios nestes tempos complexos.

Folheto

Alcatel·Lucent Enterprise

A nova realidade #WFH

Com a situação global atual, as empresas que antes não ofereciam uma opção de trabalho remoto (#WFH - work from home) são agora desafiadas a transformar as suas organizações para garantir a segurança e a continuidade dos negócios.

Em 2008, a Alcatel-Lucent Enterprise iniciou uma estratégia de trabalho a partir de casa, abraçada por mais de 50% dos 2.000 funcionários que trabalham em 50 escritórios em todo o mundo. Com mais da metade dos funcionários da ALE trabalhando em casa, já tínhamos a rede e a arquitetura de TI necessárias para suportar o trabalho remoto. O desafio era realmente uma questão de como iríamos passar de 50% de trabalhadores online para 100%.

Prontos para a ação

No início de 2017 a ALE já havia embarcado em uma extensa transformação de TI. Foi adotada uma arquitetura de rede que forneceu segurança na nuvem para bloquear ameaças de forma proativa, identificar possíveis ataques e garantir acesso seguro para os funcionários.

A transformação incluiu:

- Segurança na nuvem com pontos de acesso virtuais
- Rastreamento em tempo real
- Identificação de padrões de comportamento incomuns para detectar ameaças

Folheto
Mantenha o seu negócio seguro mesmo quando for necessário o trabalho remoto

Preparação = Resposta ágil em situações de crise

Quando a crise surgiu, a decisão de começar a trabalhar à distância na segunda-feira foi tomada na tarde da sexta-feira anterior. Os funcionários foram instruídos a levar seus notebooks e monitores para casa. Na segunda-feira de manhã o trabalho começou como sempre, sem interrupção, pois os funcionários começaram o seu dia a partir dos seus escritórios remotos. A transformação da rede realizada anteriormente assegurava a conectividade remota segura, independentemente da localização dos funcionários.

O desafio do acesso

Um dos maiores desafios que enfrentamos foi com os perfis dos usuários, incluindo as equipes de P&D e suporte técnico, que têm necessidades específicas para acessar certos servidores e plataformas de desenvolvimento, o que nossa solução de acesso remoto não permitia. Os perfis de usuários destes funcionários passaram por uma solução de acesso privado diferente do resto das equipes.

Quando o esforço de transição de todos os funcionários para #WFH começou, adaptamos nossa infra-estrutura para aumentar nossa largura de banda e suportar o aumento no número de conexões remotas exigidas pelos funcionários que trabalham a partir de casa.

A segurança é a chave

A segurança e a proteção dos dados corporativos são extremamente importantes em tempos de incerteza e afetam muitas organizações que lidam com dados sensíveis, como organizações do setor público, ministérios, cidades e vilas.

Antes mesmo de começarmos a falar de #WFH na ALE, implantamos uma infraestrutura distribuída e segura, bem como uma solução de conexão privada totalmente baseada em nuvem para todos os funcionários, a fim de garantir o acesso remoto seguro à rede. Mantemos a solução VPN existente para uma pequena porcentagem das equipes que tinham necessidades específicas, como a conexão de telefones IP nos seus escritórios remotos. Também fornecemos aos funcionários computadores profissionais, com a capacidade de gerenciar downloads e atualizações de software automaticamente.

Feche a porta para as violações de segurança

Como esperado, durante este período de trabalho remoto extensivo, houve um aumento nas chamadas e notificações relativas a e-mails suspeitos e pedidos de atualização de senha. Também temos percebido um pico nos ataques de phishing, bem como ataques direcionados a software vulnerável.

Embora o uso de proxies proteja a ALE dos principais problemas de cibersegurança, ainda vemos novas brechas todos os dias, de e-mails, downloads ou de versões não atualizadas de software/OS.

Mantenha as comunicações abertas

Na ALE, mantemos uma conexão virtual contínua com as equipes. Nós nos comunicamos regularmente, compartilhamos dicas e melhores práticas e asseguramos que nossas equipes estejam disponíveis para apoiar a todos os colaboradores.

Checklist da ALE para um trabalho remoto seguro:

- Não permita ou encoraje o uso de dispositivos pessoais (PCs) para a troca de dados e comunicações profissionais
- Permita o acesso privado e seguro dos funcionários
- Automatize atualizações de software em toda a rede corporativa
- Esteja atento às solicitações de e-mails suspeitos
- Use software certificado. As auditorias e certificações fornecem autenticação de segurança de software.
- Simplifique os seus processos de decisão. Em situações de emergência, um CISO ou CIO precisa tomar decisões rapidamente para resolver os problemas, a fim de garantir a continuidade dos serviços.

Seis recomendações da ALE para conectividade remota segura

1. Automatizar lembretes de mudança de senha

Ajude os funcionários a mudar as senhas corporativas antes que elas expirem. Antes da expiração os funcionários receberão um e-mail diário com instruções convidando-os a alterar a senha.

2. Ativar o backup de dados na nuvem

Permita e encoraje os funcionários a guardar os seus dados regularmente para evitar qualquer perda no caso de um problema com os seus computadores portáteis. Habilite espaços de armazenamento de backup de dados e ofereça assistência remota através do atendimento de TI ou especialistas em TI, conforme necessário

3. Lembrar aos funcionários sobre as melhores práticas de proteção do dispositivo

Mantenha o seu notebook em perfeitas condições:

- Desligue o notebook no final de cada dia (evite o modo de descanso/bloquear)
- Mantenha os notebook longe de fontes de calor (como o sol ou o aquecedor)
- Evite comer ou beber ao lado do notebook
- Mantenha cabos longe de crianças e animais de estimação

4. Segurança em primeiro lugar

Oriente as equipes sobre riscos e melhores práticas de segurança:

- Incentive os funcionários a pensar duas vezes antes de clicar em links em e-mails, mesmo quando parece ter sido enviado por alguém conhecido
- Ofereça acompanhamento da TI em caso de dúvidas
- Forneça ferramentas de relatório para e-mails suspeitos
- Use a gamificação para criar uma cultura de "segurança em primeiro lugar": Na ALE, usamos a gamificação para incentivar os funcionários a detectar e denunciar e-mails suspeitos

5. Comunicação

O isolamento torna as pessoas vulneráveis a ataques cibernéticos. Encontre formas de manter suas equipes conectadas:

- Organize atualizações regulares, reuniões virtuais, eventos, espaços de colaboração, happy hours
- Incentive as pessoas a se conectarem regularmente com suas equipes
- Envie e-mails regulares para informar aos funcionários que a equipe de TI está disponível para ajudá-los, e lembrá-los regularmente sobre as melhores práticas de segurança

6. Promover hábitos saudáveis de conectividade

O risco com o trabalho remoto é o mesmo de um dia de trabalho de 12 horas, com conectividade contínua ou reuniões em sequência. Incentive os funcionários a terem tempo livre longe da tela e desconectados, além de passarem mais tempo com a família ou ao ar livre.

Alcatel-Lucent Rainbow™ para uma colaboração conectada

Rainbow: uma plataforma de colaboração na nuvem para chat, chamadas de vídeo e áudio, além de compartilhamento de tela e documentos, que fornece aos funcionários da ALE as ferramentas de que eles precisam para se manterem conectados. A plataforma é amplamente usada por todos os funcionários para colaborar com os colegas.

Além disso, nossos parceiros e clientes também adotaram o Rainbow como a sua solução de colaboração. O Rainbow aborda os requisitos de segurança do setor público, defesa, cuidados de saúde e outros setores específicos e está em conformidade com rigorosos regulamentos de segurança, incluindo: GDPR, ISO 27001, HDS, entre outros.

Rainbow™

Folheto
Mantenha o seu negócio seguro mesmo quando for necessário o trabalho remoto

Apoiando a nossa comunidade

A ALE apoia os esforços de continuidade dos negócios nas empresas, cidades e governos, ajudando-os manter a continuidade segura dos serviços no ambientes de trabalho remoto. Além disso, em resposta ao aumento na demanda e no número de usuários, ampliamos nossa capacidade de hospedagem em nuvem para atender às necessidades dos clientes.

Para mais práticas de segurança cibernética, consulte as recomendações da Agência de Segurança Cibernética da UE.

Alcatel·Lucent
Enterprise