Security risk assessment report

Part 1: Select up to three hardening tools and methods to implement
Ao analisar a segurança de rede e sistemas como um todo, pode-se notar algumas inseguranças, como: 1. Os funcionários da organização compartilham senhas; 2. A senha de administrador do banco de dados está definida como padrão; 3. Os firewalls não têm regras implementadas para filtrar o tráfego que entra e sai da rede; 4. A autenticação multifatorial (MFA) não é usada; Sendo assim encontrada 4 inseguranças, que serão resolvidas com algumas ferramentas e hardening de rede, descritas logo abaixo, e uma breve descrição para pouco entendimento. Obrigatório (Para os problemas acima, APENAS): - Políticas de Senhas No caso são regras estabelecidas em um servidor(exemplo AD), onde tem que seguir as regras estabelecidas sobre a senha, senão, não consegue alterá-las assim não consegue entrar no sistema. - Multifactor authenticator (MFA): Para autenticar se a pessoa que está acessando a conta/email, é realmente a dona desse email(recomendo atrelar ao microsoft authenticator) - Manutenção do firewall: Está parte é de deveras importante para uma segurança na rede. Se algo estiver desatualizado, os atacantes podem usar isso como ponto de entrada. - Filtragem de porta: Um filtro criado em um firewall, para bloquear ou permitir certos números de porta, para limitar comunicações indesejadas. Opcional(unicamente para sua empresa, é importante ter): - Remover ou desabilitar softwares não usados de máquinas Mesmas coisa, ponto de partida de atacantes, com desatualização ou inutilização do software. - Backups de servidores, firewalls e máquinas: Se sofrer um ataque, ou algo mais comum que gera uma perda de

dados, tem algo onde dá para se reerguer.

1 vez por semana ou a cada 2 semanas:

- Pen Test:
  Um ataque ético(que não tem fins de fazer algo ruim), para descobrir vulnerabilidades do sistema. Trazendo cada vez mais proteção, pois se descoberto a vulnerabilidade às ameaças e riscos caem na probabilidade.

Existe outras coisas que são menos do que essas, mas que não se descartam, se quiserem conversar, explico mais.

Part 2: Explain your recommendations

Obrigatorio:

- Políticas de Senhas
  Neste caso a senha não será fácil de acesso. No caso, 8 ou + caracteres sendo letras e números, letra maiúscula, 2 caracteres especiais, já estava bom.
- Multifactor authenticator (MFA):
  Para autenticar se a pessoa que está acessando a conta/email, é realmente a dona desse email(recomendo atrelar ao microsoft authenticator), resolvendo o problema de outras pessoas acessando a conta de outra pessoa, ou também o problema de não ter MFA
- Manutenção do firewall:
  Isso é algo que tem que ter em tudo quanto é lugar, pois se não tiver um firewall atualizado, e de ótimo estado para uso de políticas e regras, entre outras coisas. Ele fica vulnerável, assim sua rede fica vulnerável.
- Filtragem de porta:
  Um filtro criado em um firewall, para bloquear ou permitir certos números de porta, para limitar comunicações indesejadas. No caso, criando políticas e regras de filtragem, pois agora está passando tudo em sua rede, não importa se está errado.