RANSOMWARE: PREVENÇÃO E PROTEÇÃO

PROTEÇÃO EM TEMPO REAL

O ransomware é uma ameaça crescente, uma vez que os malfeitores encontraram a forma de rentabilizar o malware, ao paralisar sistemas informáticos e exigir o pagamento de um resgate para a sua libertação. Ao contrário de outro malware, que frequentemente tem de ficar oculto durante longos períodos para funcionar eficazmente, o ransomware é criado com vista à execução rápida, através de "spear-phishing", websites comprometidos e transferências falseadas. As instituições financeiras são particularmente vulneráveis ao impacto do ransomware, porque este pode ameaçar a capacidade de mover fundos de forma rápida e eficiente, e porque são considerados alvos lucrativos. No entanto, por vezes os malfeitores não cumprem as suas promessas: mesmo após o pagamento de um resgate, alguns piratas informáticos não removem o malware ou não libertam dados confidenciais.

- Invista em sistemas de proteção anti-malware, que se adaptem às informações sobre novas ameaças em tempo real.
- Avalie a segurança de todos os dispositivos ligados a redes que contenham informações sensíveis ou essenciais. Ligue todos os sistemas não essenciais a uma rede separada.
    - Tenha especial cuidado ao trazer IoT ou "dispositivos inteligentes" para os espaços de trabalho, uma vez que estes sistemas têm frequentemente sistemas de segurança mais débeis ou inexistentes e podem ser visados como pontos de acesso a sistemas essenciais.
    - Considere a segurança de estações de trabalho remotas. Garante que as ferramentas de segurança trabalham fora da rede para monitorizar todo o tráfego Web.
- Promova a formação dos funcionários em matéria de ataques de phishing e a necessidade de ter proteções de palavras-passe fortes.
- Considere implementar a autenticação multifator em toda a sua organização, caso tal seja viável.
- Mantenha todo o software e todos os sistemas atualizados regularmente. Altere as definições para permitir atualizações automáticas, se possível.
- Desenvolva um plano de resposta a incidentes e gestão de crises para saber como lidar com um ataque de ransomware e a perda de dados valiosos.
- Prepare um plano de comunicação externa em caso de um ataque de ransomware.

CÓPIAS DE SEGURANÇA DE DADOS

- Invista em sistemas de cópia de segurança seguros e atualizados regularmente, que mantenham os seus dados protegidos.
    - Se usar USB ou discos rígidos, desligue fisicamente estes dipositivos dos computadores ligados à rede após a conclusão das cópias de segurança.
    - Se utilizar armazenamento na cloud, equipe o servidor com encriptação de alto nível e autenticação multifator.
- Crie uma cópia de apenas leitura do razão geral, para efeitos de recuperação pós-catástrofe no pior dos casos.
    - Desenvolva sistemas que realizem a recuperação e reparação automáticas de dados.
- Desenvolva cenários para avaliar quando tempo levará para recuperar dados e serviços empresariais essenciais.

AMBIENTE REGULAMENTAR

- Avalie as orientações regulamentares e jurídicas relevantes em matéria de ransomware no seu ambiente operativo.
    - Considere as orientações específicas do país. Desenvolva um plano para a avaliação periódica de orientações em mudança.
    - Considere as orientações específicas para o setor financeiro.
    - Considere os requisitos jurídicos e regulamentares de âmbito internacional.
- Avalie os riscos envolvidos no pagamento de um resgate. Em alguns casos, o pagamento de um resgate pode violar os regimes de sanções vigentes contra agentes hostis.
- Articulação com as autoridades locais de aplicação da lei. Desenvolva ligações para a partilha rápida de informação em caso de um ataque.
- Avalie as vantagens e desvantagens das apólices de seguro contra riscos cibernéticos, nomeadamente ransomware.

Avaliar a preparação da sua organização para lidar com ransomware

Considere as seguintes questões ao desenvolver um plano de prevenção e proteção contra o ransomware.

1. A sua organização tem **programadas cópias de segurança regulares?**
    - Estas cópias de segurança estão desligadas da sua rede, através de sistemas de armazenamento na cloud ou de USB/discos rígidos isolados ("air-gapped")?
2. Quaisquer **dispositivos não essenciais estão** ligados à rede da sua organização?
    - Podem ser movidas para outras redes que não contêm dados sensíveis?
3. A sua organização compreende os riscos **regulamentares e jurídicos** envolvidos no pagamento de um resgate?
    - As orientações jurídicas sobre esta matéria variam de país para país e são atualizadas frequentemente.
4. A sua organização atualiza regularmente o seu software e os seus sistemas? As atualizações são **automatizadas?**
5. A sua organização tem um **plano para lidar com um ataque de ransomware** e a perda de dados valiosos?
6. A sua organização tem uma **apólice de seguro contra riscos cibernéticos?** Em caso afirmativo, como é que esse plano cobre os ataques de ransomware?
    - Alguns planos proíbem explicitamente o pagamento de resgates, enquanto outros abrangem tais pagamentos como parte da política.

CARNEGIE ENDOWMENT FOR INTERNATIONAL PEACE
INTERNATIONAL MONETARY FUND
THE WORLD BANK IBRD • IDA | WORLD BANK GROUP
SWIFT
SWIFT INSTITUTE
FS-ISAC
Standard Chartered
CYBER READINESS INSTITUTE
GLOBAL CYBER ALLIANCE
ICBA Independent Community Bankers of America®