**FACULDADE DE TECNOLOGIA ALCIDES MAYA - AMTEC**

**CURSO TÉCNICO EM INFORMÁTICA**

LUAN LIMA KAROLCZAK

**Roubo de dados Ransomware**

Praticas para reduzir os riscos.

**Porto Alegre**

**2020**

**Resumo**

**Título:**

Roubo de dados Ransomware

Praticas para reduzir os riscos.

**Tema:**

Uso de arquiteturas de segurança para reduzir os riscos de ransonwares.

**Objetivo:**

Identificar práticas recomendadas para reduzir os riscos de ataques ransomwares, utilização de novas arquiteturas avançadas de segurança para lidar com as ameaças de ataques.

**Justificativa:**

Devido ao aumento de crimes cibernéticos que vem ocorrendo durante os últimos anos, constantemente empresas e organizações vêm sendo invadidas e acabam perdendo dados importantes, dados que na maioria dos casos estão relacionados a clientes. Com isso vamos abordar uma das ameaças que mais cresce atualmente o ransomware.

**Revisão bibliográfica:**

Ataques de ransomware vêm aumentando muito nestes últimos anos, a cada dia que passa o número de ataque só aumenta “De acordo com um relatório interinstitucional do governo dos EUA, desde janeiro de 2016, houve uma média diária de mais de 4.000.” (MILLER, 2017, P. 3). O ransomware é usado nestes ataques para roubar e criptografar os dados da vítima, por isto o ransomware é definido como um software malware, depois que o invasor consegue os dados da vítima, a mesma não tem mais acesso, sendo obrigada a pagar para resgatar seus dados.

Na maioria dos ataques funcionam da seguinte forma, os invasores infectam por malware, anúncios, sites que a empresa ou organização costuma visitar ou por e-mail através de ataques phishing.

Uma vez iniciado, o ransomware geralmente identifica os arquivos e os dados do usuário e os criptografa com algum tipo de lista de extensões de arquivos incorporadas. Ele também é programado para evitar a interação com determinados diretórios do sistema (como o diretório do WINDOWS ou certos diretórios de arquivos do programa) para garantir a estabilidade do sistema, de modo que o resgate possa ser pago após o envio não funcionar. Arquivos de locais específicos que correspondem a uma das extensões de arquivo na lista são criptografados. Caso contrário, os arquivos não serão tocados. Uma vez que os arquivos foram criptografados, o ransomware normalmente deixa uma notificação para o usuário, com instruções sobre como pagar o resgate. (MILLER, 2017, P. 8).

Para tentar reduzir os ataques existem diversas praticas que podem ser aplicadas antes, durante e depois do ataque para tentar diminuir os danos causados pelos invasores, praticas que se adotadas com antecedência podem gerar resultados positivos para empresas e organizações. Com isto antes do ataque.

Há, é claro, uma série de práticas recomendadas que as organizações podem implementar proativamente antes de se tornarem alvo de um invasor. Se os invasores não puderem estabelecer facilmente um ataque - colocando seus pés na porta, como dissemos -, eles irão procurar por uma vítima mais fácil, a menos que sua organização seja o alvo de um ataque planejado. Ataques de ransomware podem ser oportunistas, e o motivo do invasor geralmente é o ganho, com o mínimo de risco e esforço possível. Portanto, adotar uma abordagem de arquitetura para impedir que um invasor acesse sua rede é a maneira mais eficaz de quebrar a “cadeia cibernética mortal” e impedir um ataque de ransomware bem-sucedido. (MILLER, 2017, P.9)

Os invasores antes do ataque procuram saber das vulnerabilidades da organização, para depois disto começar os ataques, o que os invasores buscam nestas pesquisas é saber quase são as os aplicativos que a organização tem mais vulnerabilidade e o uso de engenharia social em usuários para tentar conseguir algumas credenciais de acesso a sistemas e softwares. Diante disto a empresa deve tomar algumas aderir a algumas práticas para evitar que isto aconteça, a primeira medida é fornecer treinamento para os usuários sobre a segurança das credenciais e dados, evitando certa forma cair em phishing, à segunda medida é verificar as vulnerabilidades de risco tanto de sistemas quanto de rede, evitando uma eventual ameaça por esta vulnerabilidade.

Se caso já estiver com uma ameaça de ataque, a organização deve tomar algumas medidas o mais rápido possível, pois quanto mais rápidos menores serão os danos causados.

As ações que você vai tomar e os esforços para remediar o problema serão diferentes dependendo da situação. No entanto, não é durante o ataque que você precisa saber qual é a capacidade de resposta da sua empresa para responder a ele. As ações de resposta ao incidente devem ser compreendidas e bem coordenadas, algo que é alcançado antes de um ataque, e devem ser bem documentadas e reproduzíveis para que você possa reconstruir um incidente após um ataque e identificar as lições aprendidas e as possíveis áreas de melhoria. (MILLER, 2017, P.14)

O que deve ser importante durante o ataque é a comunicação, pois o invasor tentara diversas formas de acesso, e a equipe de TI responsável pela área de segurança deverá ter soluções eficazes, barrando o compartilhamento de algumas informações.

Comunicação oportuna e precisa de informações a todas as partes interessadas: as informações relevantes devem ser dadas aos executivos para que recursos adequados possam ser alocados para a resposta ao problema e sua solução, de modo que se possam tomar decisões de negócios críticas e bem informadas, e para que as informações apropriadas possam, por sua vez, ser comunicadas aos funcionários, forças policiais, clientes, acionistas e público em geral.

Compartilhamento automático de novas informações de segurança por meio da arquitetura: ao coletar dados críticos de sistemas diferentes, como segurança de informações e gerenciamento de eventos (SIEM), inteligência contra ameaças e ferramentas espaciais seguras, a equipe de resposta a incidentes pode esclarecer e avaliar de forma rápida e eficaz os incidentes de segurança de alto impacto. Por exemplo, se uma nova carga de malware for detectada em um dispositivo, ela deverá ser enviada automaticamente para uma plataforma de inteligência contra ameaças na nuvem para ser analisada e para procurar e extrair possíveis indicadores de comprometimento (IoC). Depois, novas medidas corretivas devem ser implementadas e aplicadas automaticamente. (MILLER, 2017, P.14)

Depois que ocorre o ataque começa uma etapa muito importante para a organização que envolve a contenção e reparo dos danos causados pelo ataque. Com isto devesse analisar os dados do ataque para criar novos métodos de prevenir e evitar um futuro ataque, coletar dados que podem servir para uma futura auditoria policial, pois tratasse de um crime virtual. Para aumentar a segurança dos dados é importante analisar os passos que o invasor fez, para aprimorar a segurança onde há vulnerabilidade, evitando um futuro ataque pelas mesmas vulnerabilidades.

**Conclusão:**

Devido à importância dos dados que as organizações trabalham e o grande número de ataques de ransomwares nos últimos anos, tornou-se cada vez mais necessário aderir praticas consolidadas de segurança nas organizações e empresas, praticas estas que podem minimizar ou até mesmo negar os ataques. Por isto a importância de aderir e desenvolver novas práticas, também vale ressaltando o quão importante é a conscientização dos funcionários e colaboradores sobre a segurança de credenciais e dados, e sobre engenharias sócias e phishing que costumam ser o ponto inicial para invasores começarem um ataque.

**Cronograma:**

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | Dia 1° | Dia 2° | Dia 3° | Dia 4° | Dia 5° | Dia 6° | Dia 7° | Dia 6° | Dia 9° | Dia 10° |
| Titulo |  | X | X |  |  |  |  |  |  |  |
| Tema |  | X | X |  |  |  |  |  |  |  |
| Objetivo |  |  | X |  |  |  |  |  |  |  |
| Justificativa |  |  | X | X |  |  |  |  |  |  |
| Revisão bibliográfica |  |  |  | X | X | X | X | X |  |  |
| Conclusão |  |  |  |  |  |  |  |  | X | X |
| Cronograma |  |  |  |  |  |  |  |  |  | X |

**Referências Bibliográficas:**

**MILLER,** Lawrence. **Defesa contra ransomware.** Edição especial da Cisco. Hoboken, NJ: John Wiley & Sons, 2017.