UC: Network Security / Cibersegurança

TP1 Report – Simplified Risk Analysis /Análise de Risco simplificada

Students (Nº / Name):

PG53733/Catarina Pereira; PG53864/Inês Neves; PG53996/Leonardo Martins;
PG54101/Miguel Gonçalves; A89370/Rui Barbosa

Threats / Ameaças	Attacks / Ataques	Vulnerabilities / Vulnerabilidades	Valor do Risco / Risk Value
Integridade e Confidencialidade Os ataques de phishing podem comprometer tanto a integridade quanto a confidencialidade dos dados. Por exemplo, se um funcionário clicar num link malicioso e fornecer as suas credenciais de acesso, um atacante pode obter acesso não autorizado a sistemas e informações confidenciais, comprometendo a integridade dos dados. Além disso, se informações confidenciais forem divulgadas ou roubadas como resultado do phishing, a confidencialidade dos dados será comprometida.	**Ataques de Phishing** O phishing pode ser usado para obter dados e credenciais de membros ou clientes da empresa, ou até mesmo métodos e processos de funcionamento. Podendo resultar num vazamento de dados. Este ataque teria como alvo a "Corporate LAN", mais especificamente "Corporate Workstations", como ponto de entrada, mas os dados obtidos (caso sejam dados de acesso) poderiam afetar a "Control System LAN" também.	As vulnerabilidades ao phishing geralmente derivam de erros humanos. Os atacantes enviam e-mails fazendo-se passar por colegas, amigos ou empresas legítimas, com o objetivo de convencer alguém dentro da organização a clicar em links maliciosos ou instalar software malicioso. Isso inicia o processo de recolha de dados e vigilância, muitas vezes sem o conhecimento da vítima. Para mitigar esses ataques, é possível oferecer formação contra phishing aos funcionários da empresa e/ou implementar um sistema de filtragem de e-mail que identifique e bloqueie mensagens suspeitas enviadas para os endereços de email corporativos.	**Alto** O valor de risco deste ataque é alto pois pode resultar no vazamento de dados privados de funcionários ou clientes da empresa, ou de credenciais de acesso da empresa, e porque é um ataque com alta probabilidade de acontecimento.
Disponibilidade Os ataques DoS/DDoS representam uma ameaça significativa, pois podem ser lançados por indivíduos mal-intencionados ou grupos organizados com o objetivo de sobrecarregar os recursos de rede de uma empresa, tornando seus serviços inacessíveis para os utilizadores legítimos.	**Ataque DoS/DDoS** Este tipo de ataque é usado para sobrecarregar os recursos de rede de uma empresa, tornando-a inutilizável para os restantes utilizadores.	As vulnerabilidades deste tipo de ataques encontram-se nos recursos de rede de uma empresa, nomeadamente a largura de banda disponível e a capacidade de processamento dos servidores. Para mitigar estes ataques, é possível aumentar os recursos, implementar uma *firewall* capaz de filtrar tráfego indesejado, integrar protocolos de segurança e escalabilidade como *IP blacklisting e load balancing* e treinar os funcionários de modo a conseguirem identificar e resolver este tipo de ataques.	**Médio** O valor de risco deste ataque foi definido como médio pois apesar de ter uma probabilidade ligeiramente alta de acontecer, o mesmo não apresenta riscos a nenhum tipo de dados confidenciais, afetando apenas a disponibilidade do serviço.

Integridade As injeções de SQL representam uma ameaça significativa, pois os atacantes podem explorar vulnerabilidades em aplicações web para injetar comandos SQL maliciosos e comprometer a integridade dos dados armazenados no banco de dados.	**Injeções de SQL** Injeções de SQL (SQLi) é um tipo de ataque de injeção que possibilita a execução de instruções SQL maliciosas em sistemas que recorrem a bases de dados SQL. Essas instruções procuram explorar vulnerabilidades em uma aplicação web para acessar indevidamente o servidor da base de dados. Os atacantes podem utilizar a injeção de SQL para contornar as medidas de segurança da aplicação, realizando a autenticação e autorização de uma página da web ou aplicação da web, além de recuperar, adicionar, modificar e excluir registros no banco de dados SQL conforme suas intenções maliciosas. Este tipo de ataques teria como alvo a "Control System LAN", mais especificamente o "Database Server".	As vulnerabilidades dos ataques deste tipo de ataque geralmente derivam de falhas no tratamento de entradas de utilizadores em aplicações da web e no próprio acesso a tabelas e dados do SQL que o utilizador comum não deveria ter acesso (devido a uma possível má configuração nos utilizadores SQL). Essas vulnerabilidades permitem que os atacantes insiram comandos SQL maliciosos por meio de formulários da web ou outros campos de entrada. As vulnerabilidades de injeção de SQL podem ocorrer quando os desenvolvedores não validam adequadamente as entradas do utilizador ou não utilizam práticas seguras de codificação, como o uso de declarações preparadas ou mapeamento objeto-relacional. Essas falhas podem ser exploradas pelos atacantes para manipular consultas SQL, obter acesso não autorizado a dados e até mesmo comprometer a integridade do sistema da base de dados.	**Médio** As injeções de SQL foram definidas como um ataque de risco médio pois apesar de ser um ataque que pode comprometer dados importantes este ataque possui uma baixa probabilidade de ser executado.

Critical resource / Recurso crítico: (justified / justificado)

Após a nossa análise de riscos, decidimos que o recurso mais crítico seria os recursos humanos, uma vez que este é o que apresenta uma maior probabilidade de revelar informações cruciais para o funcionamento da empresa ou de revelar informações confidenciais sobre os funcionários e/ou clientes, isto por negligência ou má utilização de certas ferramentas disponíveis. Quanto maior for o acesso à informação privilegiada da vítima do ataque, maior o risco presente à empresa, tornando-se um recurso ainda mais crítico.

Security control / Controlo de segurança: (justified / justificado)

Para implementar controlos de segurança eficazes contra os ataques mencionados, sugerimos o seguinte:

- Promover a conscientização e oferecer formações em cibersegurança. Essa iniciativa visa aumentar a cautela e a expertise dos funcionários na identificação e manuseamento de e-mails de phishing e outros tipos de ataques semelhantes.
- Contratar profissionais com habilidades especializadas em cibersegurança para monitorizar possíveis ataques e implementar medidas preventivas destinadas a minimizar os riscos e os danos associados.

- Realizar auditorias e revisões regulares para garantir a conformidade com as políticas de segurança e para manter os padrões de segurança estabelecidos.
- Periodicamente, contratar um profissional para conduzir testes de penetração (PenTesting) no sistema, com o objetivo de identificar falhas de segurança e garantir que sejam corrigidas o mais rapidamente possível.

Referências

Riscos Cibernéticos: principais fatores, https://www.claranet.com/br/blog/riscos-ciberneticos-principais-fatores , acedido a 17 de fevereiro de 2024

Subodh Belgi, *Critical Infrastructure Security*, Critical Infrastructure Security by Subodh Belgi | PPT (slideshare.net) , acedido entre 14 a 17 de fevereiro de 2024, 7 de dezembro de 2017