RISCOS DE SEGURANÇA NAS REDES DE COMPUTADORES

Definições

Para identificar os riscos relacionados ao uso de uma rede de computadores, é importante conhecer algumas definições. Por conta disso, iremos nos basear na norma ABNT NBR ISO IEC 27001:2013, reconhecida mundialmente como uma referência na área de segurança. Essa norma apresenta as seguintes definições:

Conceitos de segurança da informação

Ameaça

Causa potencial de um incidente indesejado que pode resultar em danos a um sistema ou organização.

Ataque

Tudo aquilo que tenta destruir, expor, alterar, desativar, roubar, obter acesso não autorizado ou fazer uso não autorizado de um ativo.

Ativo

Qualquer coisa que tenha valor para uma pessoa ou organização. Exemplo: os dados do cartão de crédito, um projeto de uma empresa, um equipamento e até mesmo os colaboradores de uma empresa podem ser definidos como ativos humanos.

Como é possível perceber nessas definições, a **ameaça** está relacionada a algo que pode comprometer a segurança, enquanto o **ataque** é a ação efetiva contra determinado ativo.

Um incidente de segurança ocorre quando uma ameaça se concretiza e causa um dano a um ativo.

Se uma ameaça se concretizou e causou um dano, isso significa que alguma propriedade da segurança foi comprometida.

Três propriedades são tratadas como os pilares da segurança: Confidencialidade, Integridade e Disponibilidade (CID).

Além delas, outras propriedades também são importantes no contexto de segurança. A norma ABNT NBR ISO IEC 27001:2013 destaca as seguintes:

Propriedades da segurança da informação

Confidencialidade

Propriedade cuja informação não está disponível para pessoas, entidades ou processos não autorizados. A confidencialidade está relacionada ao sigilo dos dados. Somente entes autorizados podem acessá-los.

Integridade

Propriedade que protege a exatidão e a completeza de ativos. Trata-se da indicação de que o dado não foi adulterado. Exemplo: um ativo permanece intacto após ser armazenado ou transportado.

Disponibilidade

Propriedade de tornar o dado acessível e utilizável sob demanda por fontes autorizadas. Se uma pessoa ou um processo autorizado quiser acessar um dado ou equipamento, ele estará em funcionamento.

Autenticidade

Propriedade que assegura a veracidade do emissor e do receptor das informações que são trocadas. A autenticidade assegura que quem está usando ou enviando a informação é realmente determinada pessoa ou processo. Em outras palavras, garante a identidade.

Não repúdio ou irretratabilidade

Propriedade muito importante para fins jurídicos. Trata-se da garantia de que o autor de uma informação não pode negar falsamente a autoria dela. Desse modo, se uma pessoa praticou determinada ação ou atividade, ela não terá como negá-la. O não repúdio é alcançado quando a integridade e a autenticidade são garantidas.

Confiabilidade

Propriedade da garantia de que um sistema vai se comportar segundo o esperado e projetado. Exemplo: se determinado equipamento foi projetado para realizar uma operação matemática, esse cálculo será realizado corretamente.

Legalidade

Propriedade relacionada com o embasamento legal, ou seja, ela afere se as ações tomadas têm o suporte de alguma legislação ou norma. No caso do Brasil, podemos citar o Marco Civil da Internet, a Lei Geral de Proteção de Dados (LGPD) e o conjunto de normas 27.000 da ABNT.

Os mecanismos de proteção se relacionam a práticas, procedimentos ou mecanismos capazes de proteger os ativos contra as ameaças, reduzindo ou eliminando vulnerabilidades. Além disso, eles evitam que uma dessas propriedades sejam comprometidas.

Tipos de ataques

Veja as principais características dos ataques ativos e passivos.

Para haver a identificação dos riscos, será necessário entender e classificar os tipos de ataques que podem ser realizados contra uma rede de computadores.

Interligadas, as tabelas a seguir apresentam os critérios de classificação desses tipos de ataques e as suas descrições:

ATAQUES	DESCRIÇÃO	TIPOS
ATIVOS	Tentam alterar os recursos do sistema ou afetar a sua operação.	Ataques de interrupção
		Ataques de modificação
		Ataques de fabricação ou personificação
		Ataques de repetição

ATAQUES	DESCRIÇÃO	TIPOS
PASSIVOS	Tentam descobrir ou utilizar as informações do sistema sem o objetivo de afetar seus recursos.	Ataques de interceptação

CRITÉRIOS	TIPOS	DESCRIÇÃO	ATAQUES
PONTO DE INICIAÇÃO	Ataques internos (inside attack)	Realizados dentro da própria rede. O atacante e a vítima estão na mesma rede (doméstica ou corporativa).	
	Ataques externos (outside attack)	Feitos a partir de um ponto externo à rede da vítima.	
METODO DE ENTREGA	Ataques diretos	O atacante, sem a ajuda de terceiros, realiza uma ação diretamente contra a vitima.	
	Ataques indiretos	O atacante emprega terceiros, ou seja, outros usuários da rede, para que o ataque seja realizado.	

OBJETIVO	Ataques de interceptação	Buscam obter informações que trafegam a rede, atacando a confidencialidade.	Ataques passivos (predominantemente)
	Ataques de interrupção	Seu objetivo é indisponibilizar um ou mais serviços de rede sobrecarregando os sistemas, as redes ou simplesmente desligando o equipamento.	Ataques ativos
	Ataques de modificação	Ocorrem quando um atacante tem acesso não autorizado a um sistema ou a uma rede e modifica o conteúdo das informações ou as configurações de um sistema.	
	Ataques de fabricação ou personificação	Buscam quebrar, principalmente, a autenticidade de um serviço, um dispositivo ou de uma rede.	
	Ataques de repetição	Uma entidade maliciosa intercepta e repete uma transmissão de dados válida que trafega através de	

		uma rede para produzir um efeito não autorizado, como a repetição de pedidos de um item ou o processo de *login* em um ambiente.	

Etapas de um ataque

Precisamos dividir um ataque em **sete etapas** para poder analisá-lo de forma mais criteriosa:

- Reconhecimento
- Armamento (*weaponization*)
- Entrega (*delivery*)
- Exploração
- Instalação
- Comando e controle
- Ações no objetivo

Os atacantes passam a ter mais privilégios no alvo à medida que avançam nas etapas. Portanto, pelo lado da defesa, o objetivo é pará-los o mais cedo possível para diminuir o dano causado.

Vejamos a seguir cada etapa de um ataque:

Reconhecimento

Na primeira etapa, o ator da ameaça realiza uma pesquisa para coletar informações sobre o local a ser atacado. Trata-se de uma fase preparatória na qual o atacante procura reunir o máximo de informações sobre o alvo antes de lançar um ataque ou analisar se vale a pena executá-lo. As informações podem ser obtidas por meio de diversas fontes: sites, dispositivos de rede voltados para o público, artigos de notícias, anais de conferências, meios de comunicação social.

Qualquer local público é capaz de ajudar a determinar o que, onde e como o ataque pode ser realizado. O atacante escolhe alvos negligenciados ou desprotegidos, pois eles possuem a maior probabilidade de serem penetrados e comprometidos.

Armamento (*weaponization*)

Após a coleta de informações, o atacante seleciona uma arma a fim de explorar as vulnerabilidades dos sistemas. É comum utilizar a expressão *exploits* para essas armas, que podem estar disponíveis em sites na internet ou ser desenvolvidas especificamente para determinado ataque.

O desenvolvimento de uma arma própria dificulta a detecção pelos mecanismos de defesa. Essas armas próprias são chamadas de *zero-day attack*.

Após o emprego da ferramenta de ataque, espera-se que o atacante tenha conseguido alcançar seu objetivo: obter acesso à rede ou ao sistema que será atacado.

Entrega (*delivery*)

Nesta fase, o atacante entrega a arma desenvolvida para o alvo. Para essa entrega, podem ser utilizados diversos mecanismos. Eis alguns exemplos: mensagens de correio eletrônico (e-mail), mídias USB, websites falsos ou infectados, interação nas redes sociais.

O atacante pode usar um método ou uma combinação de métodos para aumentar a chance de entrega do exploit. Seu objetivo é fazer com que a arma pareça algo inocente e válido, pois ludibria o usuário e permite que ela seja entregue.

Uma prática comum para essa entrega é o uso de *phishing*. Tipicamente, são enviados e-mails com algum assunto aparentemente de interesse da vítima. Nesta mensagem, existe um link ou um anexo malicioso que serve de meio de entrega da arma na máquina alvo.

Exploração

A etapa de exploração ocorre quando o atacante, após entregar a arma, explora alguma vulnerabilidade (conhecida ou não) na máquina infectada em busca de outros alvos dentro da rede de destino. As vulnerabilidades que não são publicamente conhecidas são chamadas de *zero-day*.

No caso do emprego de *phishing*, a exploração ocorre quando o e-mail recebido é aberto e o usuário clica no link ou abre o anexo, instalando um software malicioso que infecta a sua máquina. Isso permite o controle dela por parte do autor do ataque.

A partir desse momento, o atacante obtém acesso ao alvo, podendo obter as informações e os sistemas disponíveis dentro da rede atacada. Os alvos de exploração mais comuns são aplicativos, vulnerabilidades do sistema operacional e pessoal.

Instalação

A partir da exploração da máquina realizada na fase anterior, o atacante busca instalar algum tipo de software que permita a manutenção do acesso à máquina ou à rede em um momento posterior.

Para essa finalidade, é instalado no sistema alvo um *Remote Access Trojan* (RAT). Conhecido também como *backdoor*, o RAT permite ao atacante obter o controle sobre o sistema infectado.

Pelo lado do atacante, é importante que o acesso remoto não alerte nenhum sistema de proteção e permaneça ativo mesmo após varreduras por sistemas de segurança da rede de destino.

Comando e controle

A partir do momento em que um RAT (*backdoor*) é instalado no sistema alvo, o atacante passa a ter um canal de comunicação com o software instalado no alvo.

Denominado **comando e controle**, tal canal possibilita o envio de comandos para realizar ataques na própria rede local ou para atacar a rede de terceiros, caracterizando, assim, um ataque indireto

Ações no objetivo

Quando o atacante chega à última etapa, isso é um indício de que o objetivo original foi alcançado. A partir de agora, ele pode roubar informações, utilizar o alvo para realizar ataques de negação de serviço, envio de spam, manipulação de pesquisas ou jogos on-line, entre outras atividades.

Nesse ponto, o agente de ameaças já está profundamente enraizado nos sistemas da organização, escondendo seus movimentos e cobrindo seus rastros.

É extremamente difícil remover o agente de ameaças da rede quando ele já chegou a esta fase.

Vamos analisar a noticia a seguir:

Brasil sofreu 15 bilhões de ataques cibernéticos em apenas três meses. A questão não é mais ‘o que podemos fazer se sofrermos um ataque cibernético?’, mas, sim, ‘o que podemos fazer quando sofremos um ataque cibernético?

(TECMUNDO, 2019)

Ao analisarmos o caso, percebemos a importância da análise dos riscos relacionados ao uso de uma rede de computadores sem a devida proteção.

Pesquise outras situações similares e procure perceber a intervenção dos mecanismos de proteção nesses casos.