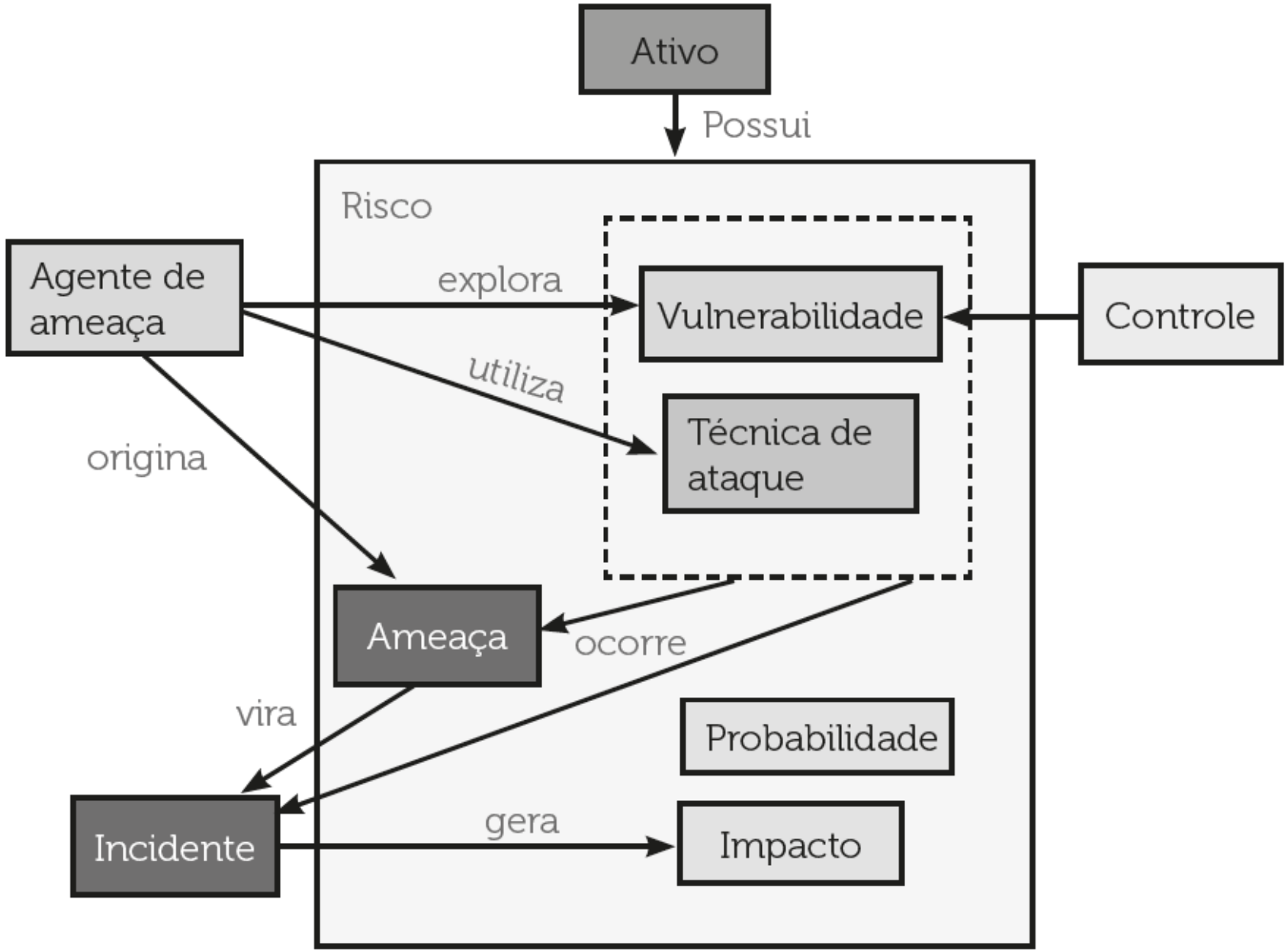
Segurança da Informação

Aula7 – Fatores de Risco

Curso de Ciência da Computação

Prof. Dr. Rodrigo Xavier de Almeida Leão

Figura 4.1 | Os elementos do risco em segurança da informação



Um agente de ameaça, que é aquele que provoca um incidente de segurança, pode ser humano, tecnológico ou a própria natureza. Quando um agente de ameaça explora uma vulnerabilidade de um ativo, uma ameaça se torna um incidente de segurança. A ameaça, assim, é algo que "está no ar", que sempre existe e pode virar um evento. Já as vulnerabilidades existem nos ativos, que podem ser humanos, tecnológicos ou físicos.

Aspectos não tecnológicos em segurança da informação

Iremos discutir três categorias gerais de aspectos não tecnológicos (ISO 27001, 2013; ISO 27005, 2011; ITU, 2003; NAKAMURA; GEUS, 2007):

- Aspectos físicos: envolvem elementos do risco que possuem características físicas, tais como data center, servidor ou localização.
- Aspectos humanos: envolvem elementos do risco que possuem características humanas, tais como administrador de sistemas, concorrentes ou *crackers*. Além disso, temos falhas e acidentes.
- Aspectos naturais: envolvem elementos do risco que possuem características naturais, tais como enchentes, terremotos ou altas temperaturas.

Ação maliciosa, não intencional ou natural?

Quem realiza uma ação é o agente e, no caso de segurança da informação, quem explora uma vulnerabilidade é o agente de ameaça. O agente de ameaça pode exercer ou provocar ações de três formas gerais (ISO 27001, 2013; ISO 27005, 2011; ITU, 2003; NAKAMURA; GEUS, 2007):

- Ação maliciosa: algo intencional, como uma invasão, um roubo ou uma destruição.
- Ação não intencional: algo não intencional, como uma falha, engenharia social ou acidente.
- Ação natural: algo que advém da natureza, como terremoto, enchente ou congelamento.

O interessante é a visão que pode ser dada para cada elemento analisado. Por exemplo, no caso de uma ação maliciosa, um roubo (ameaça) é cometido por um ladrão (agente de ameaça), que explora uma vulnerabilidade (porta aberta) de uma casa (ativo). Já no caso de uma ação não intencional, um administrador de rede (ativo) pode ser enganado por engenharia social (ameaça), por um *cracker* (agente de ameaça) que explora a ingenuidade (vulnerabilidade) dele.

No caso do exemplo da ação maliciosa, há aspectos físicos (casa como ativo) e humanos (ladrão como agente de ameaça) envolvidos. Já no caso do exemplo da ação não intencional, há somente aspectos humanos envolvidos, com seres humanos sendo o ativo (administrador de rede) e o agente de ameaça (cracker).

Já em outro exemplo de ação natural, o congelamento (ameaça) de um sistema de supressão de incêndio (ativo) pode ser causado por baixas temperaturas (agente de ameaça).

Desastres

A ideia relacionada a desastres é que ela constitui uma das piores consequências que pode existir. Portanto, sendo uma consequência, no linguajar do risco, o desastre é um dos possíveis impactos que uma empresa pode ter. De acordo com essa interpretação, um desastre pode ser tanto resultado de um ataque de *cracker*, como pode também ser resultado de um terremoto. Nessa interpretação do desastre, o valor da gestão de riscos é bastante grande, pois mostra que, para uma empresa, um ataque de *cracker* pode ser um desastre, enquanto para outra empresa o mesmo ataque pode ser apenas um infortúnio.

Alguns fenômenos naturais que podem ser considerados são:

- Enchentes e inundações.
- Terremotos.
- Altas temperaturas.
- Baixa umidade.
- Explosão solar.
- Furacão, tornado, tufão, microexplosão.

Exemplificando

Em um hipotético caso de ataque DoS, os serviços de uma empresa digital ficam interrompidos por 1 minuto. O que isso significa para a empresa? Pode haver prejuízos que, no entanto, ficam limitados pelo restabelecimento dos serviços em 1 minuto. O que ocorre se o ataque perdura não por 1 minuto, mas por 2 horas? Os impactos seriam gigantescos, mas será que isso seria um desastre? E se o ataque perdurar por mais de 24 horas? Para algumas empresas, as 24 horas de indisponibilidade podem representar um desastre. Porém, para outras, o único minuto sem os serviços pode representar também um desastre, como no caso de vidas humanas, por exemplo.

https://setorsaude.com.br/ataque-cibernetico-pode-ter-causado-uma-perda-de-us-16-bilhao-ao-grupo-unitedhealth-nos-eua/

Neste ponto, há um conceito importante em segurança da informação e avaliação de riscos: a reação em cadeia. A avaliação deve levar em consideração não apenas eventos isolados, mas também toda a sequência de eventos. Em um exemplo, o roubo da senha de e-mail do presidente da empresa, por exemplo, pode ser avaliado como sendo de um determinado nível de risco. Porém, o roubo da senha de e-mail pode ser apenas o início de um ataque maior, iniciando a reação em cadeia. O *cracker* poderia, por exemplo, se passar pelo presidente da empresa e solicitar as senhas dos servidores que armazenam os dados de todos os clientes. A partir desse acesso, o vazamento dos dados poderia levar à perda de clientes, processos judiciais e à perda de reputação.

Falhas

As falhas, sejam elas humanas ou tecnológicas, também devem ser consideradas, pois podem afetar as propriedades básicas da segurança da informação, confidencialidade, integridade e disponibilidade (ISO 27001, 2013; ISO 27005, 2011; ITU, 2003; NAKAMURA; GEUS, 2007).

As falhas humanas podem ser causadas por diversos fatores, tais como cansaço ou desatenção. O que devemos considerar, no entanto, é que diferentes ativos poderão ser afetados com uma falha humana. Por exemplo, uma informação confidencial pode ser divulgada sem intenção após uma falha na configuração do servidor, afetando a confidencialidade.

Além da falha humana, sistemas também podem falhar, o que é intrínseco, principalmente em hardware. Uma falha em um disco rígido, por exemplo, pode levar à perda de informações, com a disponibilidade sendo afetada.

Outro tipo de falha que afeta a segurança da informação é a de infraestrutura, como a elétrica. O sistema elétrico pode causar variações elétricas capazes de danificar hardware ou corromper informações, que podem afetar a disponibilidade ou a integridade.

Outra técnica de engenharia social bastante utilizada é a realização de ligações telefônicas para centros de relacionamento de serviços diversos, de posse de algumas informações sobre a vítima. Informações críticas podem ser obtidas nessas ligações, como as que foram descobertas em ataque contra um jornalista da revista norte-americana *Wired*. Nesse incidente, o *cracker* utilizou informações cruzadas de diferentes serviços da vítima para roubar a sua conta. Primeiro, ele ligou para a *Amazon* pedindo para adicionar um novo cartão de crédito. A validação foi feita com informações de nome completo, e-mail e endereço de cobrança. Em uma nova ligação, o *cracker* alegou não estar conseguindo o acesso com seu e-mail, e conseguiu cadastrar um novo utilizando informações de nome, endereço de cobrança e cartão de crédito (que ele tinha acabado de cadastrar). Com o novo endereço de e-mail cadastrado, o fraudador recuperou a senha usando o método tradicional (esqueci minha senha). Já na conta da *Amazon*, o fraudador teve acesso aos quatro últimos dígitos do cartão de crédito da vítima, que eram, por sua vez, utilizados para verificação de conta da Apple. Com o acesso à conta do *iCloud*, o fraudador conseguiu recuperar a senha do *Gmail* para depois conseguir a senha do *Twitter* (ARRUDA, 2012).

- Aspectos físicos: envolvem elementos do risco que possuem características físicas, tais como data center, servidor ou localização.
- Aspectos humanos: envolvem elementos do risco que possuem características humanas, tais como administrador de sistemas, concorrentes ou *crackers*. Além disso, temos falhas e acidentes.
- Aspectos naturais: envolvem elementos do risco que possuem características naturais, tais como enchentes, terremotos ou altas temperaturas.