1.Ameaça

Uma *ameaça* é um perigo em potencial para um ativo, como dados ou a própria rede. É o potencial de alguém ou alguma coisa explorar uma vulnerabilidade e causar uma violação de segurança. As ameaças podem ser naturais, humanas ou causadas por erros não intencionais. A pessoa ou coisa que representa uma ameaça é chamada de ***agente de ameaça***.

1.1 Nation-state

São grupos patrocinados por governos que realizam ataques cibernéticos contra outras nações, organizações ou indivíduos. Utilizam técnicas avançadas, como APTs (*Advanced Persistent Threats*), espionagem e sabotagem. Seus alvos podem incluir infraestrutura crítica, defesa, indústrias estratégicas e políticos.

- **Motivos:** Espionagem, sabotagem, guerra cibernética, roubo de propriedade intelectual.
- **Atributos:** Recursos vastos, ataques sofisticados, operações persistentes e furtivas, alvos estratégicos

1.2 Unskilled attacker

São indivíduos com pouco conhecimento técnico que utilizam ferramentas automatizadas ou exploits prontos, sem realmente entender como funcionam. Seus ataques costumam ser fáceis de identificar e conter, mas ainda podem causar danos se explorarem vulnerabilidades conhecidas.

- **Motivos:** Diversão, fama, aprendizado, desafio pessoal.
- **Recursos:** Pouco conhecimento técnico, uso de ferramentas prontas, ataques de baixo impacto, fácil detecção.

1.3 Hacktivist

Atuando por razões ideológicas, hacktivistas realizam ataques cibernéticos para promover causas políticas, sociais ou ambientais. Utilizam técnicas como *defacement* (alteração de sites), vazamento de dados e ataques de negação de serviço (DDoS). Grupos como Anonymous são exemplos de hacktivismo.

- **Motivos:** Ideologia, ativismo político/social, protestos digitais.
- **Recursos:** Motivação forte, uso de DDoS, defacement, vazamento de dados, pode variar de amador a altamente capacitado.

1.4 Insider threat

Funcionários, ex-funcionários ou prestadores de serviço podem representar riscos de segurança ao usar seus acessos privilegiados para roubo de dados, sabotagem ou espionagem. Essas ameaças são difíceis de detectar, pois partem de dentro da organização e podem envolver tanto ações intencionais quanto descuidos.

- **Motivos:** Vingança, lucro, coerção, insatisfação.
- **Recursos:** Acesso privilegiado, conhecimento interno da organização, difícil detecção, impacto potencialmente alto.

1.5 Organized crime

Grupos criminosos especializados em fraudes financeiras, ransomware, tráfico de dados e extorsão digital. Operam como verdadeiras empresas, com divisão de funções e financiamento para aprimorar seus ataques. O foco principal é o lucro, muitas vezes explorando técnicas como phishing, engenharia social e ataques avançados contra empresas e indivíduos.

- **Motivos:** Lucro financeiro, extorsão, fraude.
- **Recursos:** Estrutura hierárquica, ataques sofisticados (ransomware, phishing, lavagem de dinheiro), operações de longo prazo

1.6 Shadow IT

Refere-se ao uso não autorizado ou não gerenciado de tecnologia, sistemas, aplicativos e serviços por parte dos funcionários em uma organização. A presença de Shadow IT pode criar riscos significativos de segurança e conformidade. Portanto, as políticas de pessoal relacionadas ao Shadow IT devem abordar esse problema de forma eficaz.

As políticas de pessoal precisam estabelecer métodos para identificar o uso não autorizado de tecnologia. Isso pode incluir o monitoramento de redes, auditorias de sistemas e a análise de registros de atividades para detectar dispositivos e aplicativos não aprovados.

A organização deve definir claramente as consequências do uso não autorizado da tecnologia. Varia de ações disciplinares a medidas corretivas. Além disso, as políticas devem incluir esforços educacionais para conscientizar os funcionários sobre os riscos associados à Shadow IT.

A política deve incluir uma avaliação abrangente de riscos relacionados à Shadow IT, identificando possíveis ameaças à segurança, privacidade e conformidade, ajudando a priorizar os esforços de mitigação. As políticas devem estabelecer procedimentos claros para a autorização e supervisão de tecnologias e aplicativos antes de serem usados pelos funcionários, considerando revisões de segurança e conformidade antes da aprovação. As políticas devem incluir programas de treinamento para educar os colaboradores sobre os riscos da Shadow IT e a importância de seguir as políticas e diretrizes estabelecidas.

A Shadow IT é dinâmica, e novas tecnologias podem surgir a qualquer momento. Portanto, as políticas de pessoal devem enfatizar a necessidade de

monitoramento contínuo e adaptação às mudanças na paisagem de tecnologia para mitigar os riscos.