TP1: Análise de Risco Simplificada
Cibersegurança

Introdução

A Segurança da Informação pode ser definida como o processo conducente ao estabelecimento de um determinado nível de **confiança**, sobre um conjunto de propriedades consideradas relevantes. É quase universalmente aceite que, neste contexto, algumas propriedades são fundamentais, i.e., a confidencialidade, a integridade e a disponibilidade, não obstante outras possam ser igualmente importantes.

Um nível de confiança é traduzido por uma medida bastante subjetiva, dado o carácter pessoal do julgamento envolvido, que se traduz na perceção do **risco**. Claramente, diferentes indivíduos considerarão aceitáveis diferentes níveis de risco e, consequentemente, o seu nível de confiança será diferente.

Apesar desta evidente causa de disparidade na perceção da segurança, existem modelos simples que permitem traduzir o nível de risco e que são fundamentais para conseguir planear conscientemente uma infraestrutura de segurança. Um desses modelos baseia-se na determinação do risco (**R**) como sendo o produto do **valor do sistema em causa** pela **probabilidade de ocorrência de um evento** danoso:

$$R = V \times P$$

Dependendo do recurso em causa, o valor (**V**) pode corresponder a um valor material facilmente calculado, pode ser deduzido do impacto da perda (total ou parcial) do sistema, ou pode corresponder a um valor mais indefinido, como seja o valor de uma marca ou de uma informação (este tópico não será aqui considerado, por se enquadrar mais no âmbito da disciplina de Gestão do Risco).

Por seu lado, a probabilidade (**P**) da ocorrência de um evento danoso estará associada à(s) **vulnerabilidade(s)** existente(s) no sistema e que permitirá(ão) essa ocorrência, à(s) **ameaça(s)** pendentes sobre o sistema e que pode(m) desencadear o evento e ao(s) **ataque(s)** que poderá(ão) causar o evento. Sendo assim, numa perspetiva simplista da questão da segurança num Sistema de Informação, a abordagem segundo este modelo indica que deveremos começar por estudar as vulnerabilidades, as ameaças e os possíveis ataques (não necessariamente por esta ordem). Só depois desse exercício e usando o valor dos recursos em questão, poderemos avaliar o risco e tomar as decisões acertadas quanto às medidas de segurança (ou controlos de segurança) a implementar, para atingir um certo nível de segurança.

Objetivos

No final deste trabalho deverá estar apto a:

1) Identificar ameaças, ataques e vulnerabilidades numa rede de computadores e na respetiva infraestrutura informática.
2) Explicar a diferença entre ameaça, ataque e vulnerabilidade.
3) Estimar o índice de risco, com base na análise das ameaças, ataques e vulnerabilidades.
4) Identificar algumas medidas básicas para a Segurança da Informação.

Material

Suponha que trabalha numa Infraestrutura Crítica (IC), para onde foi contratado como CSO (*Chief of Security Officer*). Como primeira tarefa é-lhe pedido que realize uma análise de segurança da informação direcionada a toda a infraestrutura de processamento e comunicações, com o objetivo de identificar as vulnerabilidades, as ameaças e os possíveis ataques. Numa primeira aproximação é-lhe dito que a infraestrutura tecnológica corresponde a uma arquitetura típica, como aquela que é mostrada

na Figura 1, integrando componentes convencionais[1] dos Sistemas de Informação (*Corporate LAN*, na figura), com a tecnologia específica de controlo de sistemas industriais (*SCADA Network*, na figura) e os componentes distribuídos implantados junto dos equipamentos específicos da infraestrutura em causa (*Field Devices*, na figura - RTU, IED, PLC, etc.), tudo isso interligado. Encontra uma descrição simples deste tipo de arquitetura aqui (siga o *link*).

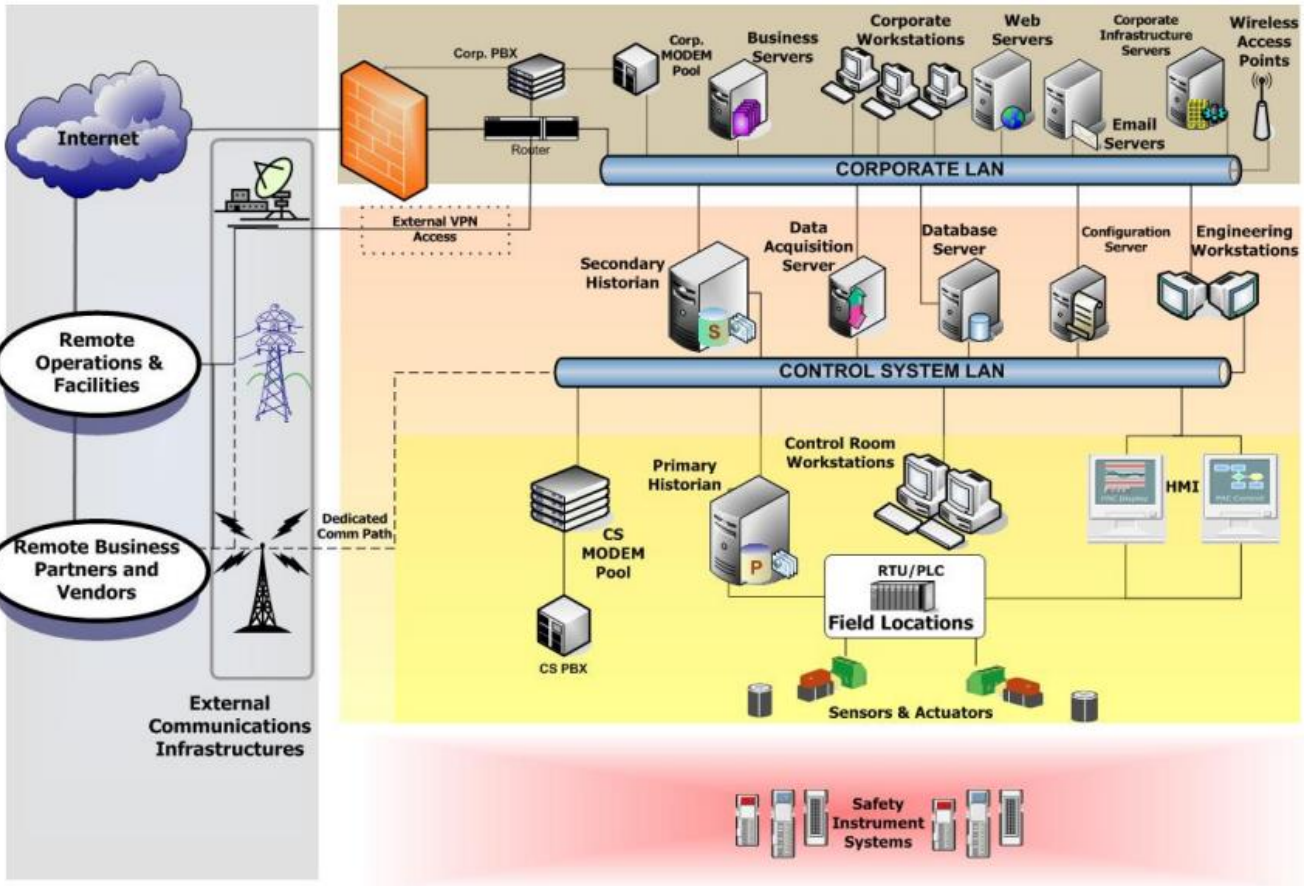

Figura 1– Arquitectura típica do sistema de informação de uma infraestrutura crítica (ICS)[2]

Na execução do trabalho poderá ainda ser-lhe útil a leitura do capítulo 1 dos livros "Cybersecurity: Engineering approach" e "Security in Computing", referenciados na bibliografia da UC.

Tarefas

Analisando a Figura 1 e a descrição associada (ver o *link* acima indicado), indique, numa tabela:

1. Três **ameaças** que considera relevantes (que se traduzem em um maior risco).
2. Um ou mais **ataques** associados a cada uma das ameaças.
3. As **vulnerabilidades** que são exploradas em cada ataque.
4. Uma estimativa do valor do risco, para cada um dos casos; mais do que um valor absoluto, interessa estabelecer valores relativos entre os casos considerados.

Indique ainda qual o **recurso** que, na sua opinião, evidencia o **maior risco** e justifique a sua escolha. Finalmente, identifique um controlo de segurança que procure atenuar esse risco.

Nota: Embora o trabalho sugira que comece por identificar as ameaças, poderá começar por identificar ataques, ou mesmo vulnerabilidades; o importante é que cada linha da tabela seja coerente.

[1] Por componentes convencionais entenda-se o conjunto de computadores pessoais (portáteis ou estações de trabalho, servidores, impressoras e equipamento de rede de comunicações necessário para implementar redes locais.
[2] Extraído de [1]. Este artigo apresenta um interessante trabalho sobre a proteção deste tipo de sistema.

Bibliografia adicional:

[1] CSSP, DHS. "Recommended Practice: Improving Industrial Control Systems Cybersecurity with Defense-In-Depth Strategies." *US-CERT Defense In Depth (October 2009)* (2009).
[2] Janicke, Helge, et al. "Runtime-Monitoring for Industrial Control Systems."*Electronics* 4.4 (2015): 995-1017