EgoInc - Plano de Segurança

Citeforma | CET 8493 | UFCD 9194 Cibersegurança e Ciberdefesa | Formador: João Almeida

Hugo Miguel Félix Bugalho | João Rodrigo Mota da Costa

Introdução

Desde a fundação da **Ego Incorporated** que o nosso foco tem sido a cibersegurança. Como qualquer empresa desta área, queremos ser um nome em que toda a gente confia. De empresas, a colaboradores, a trabalhadores independentes, damos sempre o nosso melhor para dar as infraestruturas mais convenientes e seguras, com apoio e formação de topo.

Com o confinamento e complicações devido à pandemia, a procura e oportunidade para mostrar todas as ferramentas ao nosso dispor reduziu, e as reuniões e formações à distância foram um percalço na nossa missão. Mas pelo mesmo vetor, as tecnologias que nós e os atacantes do ciberespaço utilizam evoluíram de forma substancial: De novas vulnerabilidades, a ferramentas serem desenvolvidas para abusar das mesmas, tudo para serem divulgadas a cada vez mais pessoas que as podem usar para efeitos maliciosos.

Este documento surge para mostrar quais são os planos da **EgoInc** para o futuro, com um foco especial em melhorar a nossa formação para todos os nossos colaboradores sobre ataques de vetor físico com a entrada de muitos de nós na nossa sede, situada no Monte da Barrasqueira.

Objetivos e resultados pretendidos

Objetivos

Um dos maiores objetivos da **EgoInc** é estabelecer uma relação de confiança com todos os nossos clientes. Tentamos oferecer as melhores estruturas e processos de configuração de sistemas de proteção informática, fazemos auditorias a infraestruturas informáticas, análise e gestão de riscos cibernéticos, simulações de ataque e defesa e ações de formação a todos os nossos colaboradores e clientes.

Estratégia de cibersegurança

Mais formações relativos a ataques de *phishing* e *social engineering*; Implementar medidas de segurança para a sala dos servidores; Implementar métodos de autenticação; Maior gestão no controlo de credenciais.

Âmbito e responsabilidades

Âmbito

A ambição da **EgoInc** é a credibilidade e a transparência para com os nossos colaboradores e clientes. Somos grandes apoiantes do movimento de *software* gratuito e de código livre (ou *FOSS - Free and Open Source Software*)

Responsabilidades

As nossas responsabilidades são garantir a segurança e privacidade dos nossos clientes no ciberespaço com o máximo de conveniência possível. Isso inclui o cumprimento de regras e políticas impostas a todos os colaboradores, incluindo o núcleo administrativo e melhoramentos constantes aos nossos sistemas.

Requisitos e objetivos de cibersegurança

Sistema atual

Atualmente a *EgoInc* dispõe de um sistema de redundância com parte física e parte virtualizada, alojada na *cloud*. Para além da configuração normal de rede (Router, Switch e Firewall), a *EgoInc* tem dois servidores físicos com redundância, o principal em Rocky Linux e o backup em Windows Server 2003. Na *cloud*, está alojado no Linode um servidor de backups contra ataques de *ransomware*, e na OVH-Cloud um sistema de máquinas virtuais para simulação de ataques informáticos remotos.

Ferramentas e políticas de cibersegurança existentes

Na **EgoInc**, fazemos alguns esforços para garantir a segurança dos nossos colaboradores e a privacidade dos nossos clientes.

Para esses efeitos, implementamos a "política das mesas limpas", em que pedimos aos colaboradores para não abandonar os seus postos de trabalho com qualquer tipo de documentação confidencial de forma visível, quer para a empresa ou para os nossos clientes. A recomendação feita foi para guardar os documentos nas gavetas das secretárias dos postos de trabalho, preferencialmente fechados à chave, antes de abandonar o posto para qualquer efeito lúdico ou empresarial.

Apesar de a EgoInc encorajar os colaboradores a personalizar o seu espaço, pedimos que não ocupem demasiado espaço com itens pessoais. No caso dos colaboradores quererem salvaguardar os seus pertences, têm disponíveis cacifos para o efeito.

Regulamentos, normas e boas práticas

Em qualquer empresa focada na área da segurança, deve haver regulamentação relativamente à política de BYOD *(Bring Your Own Device)*. No caso da **EgoInc**, nós tornamos explicitamente

proibido o uso de equipamentos e dispositivos pessoais para o contexto profissional. Apesar de isto incluir um custo mais caro para compra e manutenção de máquinas, é um custo necessário para certificar consistência e qualidade para os nossos clientes. Todos os nossos colaboradores têm um posto de trabalho dedicado na nossa sede e para os colaboradores que necessitam de fazer trabalho remoto ou diretamente num cliente estão equipados com portáteis da gama Thinkpad da Lenovo e telefones da linha Pixel da Google com o Graphene OS, para certificar uma experiência segura e sem telemetria.

Outra regra que planeamos implementar no futuro é a proibição da utilização de dispositivos USB externos, quer dentro como fora da sede da **EgoInc**, optando por apenas utilizar os dispositivos USB permitidos pelo departamento de IT, como *pens* e discos externos. Esta regra tem o propósito de evitar a propagação de *malware* e outros programas não autorizados dentro das nossas infraestruturas. Caso os colaboradores necessitem de um dispositivo USB, pode ser requisitado ao departamento de IT e devolvido após a sua utilização. Pode ser considerado uma opção excessiva, mas ao reduzir a nossa superfície de ataque evitamos ataques "desnecessários", mas que podem causar milhões de euros em danos.

Pontos de entrada

Os pontos de entrada na sede da **EgoInc** são os seguintes:

- Entrada da sede, situado no Monte da Barrasqueira;
- Receção para visitantes;
- Entrada para o interior do edifício com controlo de entrada e saída (torniquete e sistema informático);
- Sala dos servidores com segundo método de autenticação para pessoal autorizado;

Controlos de cibersegurança

Nenhuma empresa está imune a ataques, quer seja por vetor físico ou virtual. Para controlo de cibersegurança, a **Negocio** utiliza os seguintes métodos:

- Auditoria física ao interior do edifico, feito bianualmente
- Auditoria remota à infraestrutura informática, feito bianualmente
- Teste de penetração física, feito anualmente

Para todos estes controlos são utilizadas empresas diferentes para comprovar a nossa segurança e qualidade para os nossos clientes.