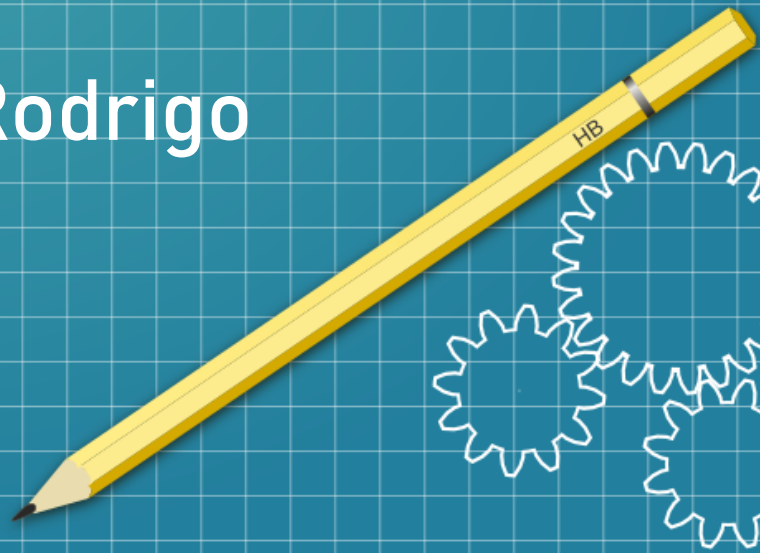
EgoInc

Introdução à Cibersegurança e Ciberdefesa

Hugo Bugalho | João Rodrigo



O que é a EgoInc?

Localização: Monte da Barrasqueira

Serviços:
- Configuração de sistemas de proteção informática
- Auditorias a infraestruturas informáticas
- Análise e gestão de riscos cibernéticos
- Simulações de ataque e defesa
- Ações de formação

O que é a EgoInc?

Infraestrutura:

Sistema de rede (router, switch e firewall)
Dois servidores físicos (Rocky Linux e Windows Server 2003)
Dois servidores na cloud (Linode e OVH-Cloud)

Responsáveis de segurança

Nome da entidade	Nome do responsável de segurança	Cargo do responsável de segurança	Endereço de correio eletrónico	Número de telefone fixo (se aplicável)	Número de telefone móvel
Ego Incorporated	Rebeca Rodrigues Roque	Chief Information Security Officer (CISO)	rrr@ego.inc	(+351) 21 217 1508	(+351) 92 128 3576
Ego Incorporated	Jikutoku Mitakafuchimoto	Técnico Operacional	jikutoku@ego.inc	(+351) 21 265 5047	(+351) 91 369 2037

Pontos de contacto permanente

Nome da entidade	Nome do ponto ou pontos de contacto permanente / serviço disponível ou equipa operacional	Endereço de correio eletrónico principal	Endereço de correio eletrónico alternativo	Número de telefone fixo principal (se aplicável)
Ego Incorporated	Takuku Katotoku	takuku@ego.inc	t.katotoku@armyspy.com	(+351) 21 069 0420
Ego Incorporated	Luís Ribeiro Ferreira	l.ferreira@ego.inc	LuisRibeiroFerreira@teleworm.us	(+351) 21 069 0420

Número de telefone móvel principal	Número de telefone fixo alternativo (se aplicável)	Número de telefone móvel alternativo	Outros contactos alternativos	
(+351) 94 420 6900	(+351) 21 234 3885	(+351) 91 842 9178	Slack: Taknottem	
(+351) 94 420 6969	(+351) 21 210 2427	(+351) 96 381 4729	Slack: Cargay	

Ameaças

Ego Incorporated - Ameaças aos ativos da organização											
Serviço	Dono do ativo	Confidencialidade	Integridade	Disponibilidade	Impacto financeiro	Impacto no titular dos dados	Tipo de ameaça	Ameaça	Vulnerabilidade	Probabilidade	Impacto
Servidor 1	EgoInc	4	3	3	5	2	Espionagem Industrial	Perda de clientes	Investigaçao de candidatos	2	3
Servidor 1	EgoInc	5	5	1	4	3	Uso não autorizado de equipamento	Inactividade de serviços	Controlo do acesso	4	2
Servidor 1	EgoInc	3	3	3	4	4	Fogo	Perda equipamentos	Rede elétrica velha	2	1
Servidor 1	EgoInc	2	2	3	3	3	Bugs de software	Fraca performance	Software desatualizado	5	1
Servidor 1	EgoInc	4	4	3	5	2	Ataques de vírus	Inactividade de serviços	Falta cibersegurança	1	2
Servidor 1	EgoInc	5	4	4	3	4	Roubo de informação	Perda de dados	Falta cibersegurança	5	3
Servidor 1	EgoInc	5	1	1	3	5	Terrorismo	Perda equipamentos	Falta de segurança fisica	2	3
Servidor 1	EgoInc	4	4	1	4	1	Social Engineering	Perda de credibilidade	Formaçao	3	4
Servidor 1	EgoInc	5	2	1	1	4	Falha de energia	Inactividade de serviços	Falta gerador	3	3
Servidor 1	EgoInc	4	2	1	4	2	Falha de comunicações	Fraca performance	Apenas um provedor	2	5
Servidor 1	EgoInc	4	5	4	5	1	Corrupçao de dados	Perda de credibilidade	Dados fornecidos errados	2	3
Servidor 1	EgoInc	2	3	3	1	4	Inundações	Perda equipamentos	Servidor na cave	3	1
Servidor 2	EgoInc	4	3	3	5	2	Espionagem Industrial	Perda de clientes	Investigaçao de candidatos	2	3
Servidor 2	EgoInc	5	5	1	4	3	Uso não autorizado de equipamento	Inactividade de serviços	Controlo do acesso	4	2
Servidor 2	EgoInc	3	3	3	4	4	Fogo	Perda equipamentos	Rede elétrica velha	2	1
Servidor 2	EgoInc	2	2	3	3	3	Bugs de software	Fraca performance	Software desatualizado	5	1
Servidor 2	EgoInc	4	4	3	5	2	Ataques de vírus	Inactividade de serviços	Falta cibersegurança	1	2
Servidor 2	EgoInc	5	4	4	3	4	Roubo de informação	Perda de dados	Falta cibersegurança	5	3
Servidor 2	EgoInc	5	1	1	3	5	Terrorismo	Perda equipamentos	Falta de segurança fisica	2	3
Servidor 2	EgoInc	4	4	1	4	1	Social Engineering	Perda de credibilidade	Formaçao	3	4
Servidor 2	EgoInc	5	2	1	1	4	Falha de energia	Inactividade de serviços	Falta gerador	3	3
Servidor 2	EgoInc	4	2	1	4	2	Falha de comunicações	Fraca performance	Apenas um provedor	2	5
Servidor 2	EgoInc	4	5	4	5	1	Corrupção de dados	Perda de credibilidade	Dados fornecidos errados	2	3
Servidor 2	EgoInc	2	3	3	1	4	Inundações	Perda equipamentos	Servidor na cave	3	1
Cloud 1	OVH-Cloud	4	3	3	5	2	Espionagem Industrial	Perda de clientes	Investigaçao de candidatos	2	3
Cloud 1	OVH-Cloud	5	5	1	4	3	Uso não autorizado de equipamento	Inactividade de serviços	Controlo do acesso	4	2
Cloud 1	OVH-Cloud	3	3	3	4	4	Fogo	Perda equipamentos	Rede elétrica velha	2	1
Cloud 1	OVH-Cloud	2	2	3	3	3	Bugs de software	Fraca performance	Software desatualizado	5	1
Cloud 1	OVH-Cloud	4	4	3	5	2	Ataques de vírus	Inactividade de serviços	Falta cibersegurança	1	2
Cloud 1	OVH-Cloud	5	4	4	3	4	Roubo de informação	Perda de dados	Falta cibersegurança	5	3
Cloud 1	OVH-Cloud	5	1	1	3	5	Terrorismo	Perda equipamentos	Falta de segurança fisica	2	3
Cloud 1	OVH-Cloud	4	4	1	4	1	Social Engineering	Perda de credibilidade	Formaçao	3	4
Cloud 1	OVH-Cloud	5	2	1	1	4	Falha de energia	Inactividade de serviços	Falta gerador	3	3
Cloud 1	OVH-Cloud	4	2	1	4	2	Falha de comunicações	Fraca performance	Apenas um provedor	2	5
Cloud 1	OVH-Cloud	4	5	4	5	1	Corrupção de dados	Perda de credibilidade	Dados fornecidos errados	2	3
Cloud 2	Linode	2	3	3	1	4	Inundações	Perda equipamentos	Servidor na cave	3	1
Cloud 2	Linode	4	3	3	5	2	Espionagem Industrial	Perda de clientes	Investigaçao de candidatos	2	3
Cloud 2	Linode	5	5	1	4	3	Uso não autorizado de equipamento	Inactividade de serviços	Controlo do acesso	4	2
Cloud 2	Linode	3	3	3	4	4	Fogo	Perda equipamentos	Rede elétrica velha	2	1
Cloud 2	Linode	2	2	3	3	3	Bugs de software	Fraca performance	Software desatualizado	5	1
Cloud 2	Linode	4	4	3	5	2	Ataques de vírus	Inactividade de serviços	Falta cibersegurança	1	2
Cloud 2	Linode	5	4	4	3	4	Roubo de informação	Perda de dados	Falta cibersegurança	5	3
Cloud 2	Linode	5	1	1	3	5	Terrorismo	Perda equipamentos	Falta de segurança fisica	2	3
Cloud 2	Linode	4	4	1	4	1	Social Engineering	Perda de credibilidade	Formaçao	3	4
Cloud 2	Linode	5	2	1	1	4	Falha de energia	Inactividade de serviços	Falta gerador	3	3
Cloud 2	Linode	4	2	1	4	2	Falha de comunicações	Fraca performance	Apenas um provedor	2	5
Cloud 2	Linode	4	5	4	5	1	Corrupção de dados	Perda de credibilidade	Dados fornecidos errados	2	3
ISP 1	Vodafone	4	2	1	1	4	Falha de comunicações	Inactividade de serviços	Perda de credibilidade	2	2
ISP 2	MEO	4	5	5	5	4	Falha de comunicações	Inactividade de serviços	Perda de credibilidade	2	5

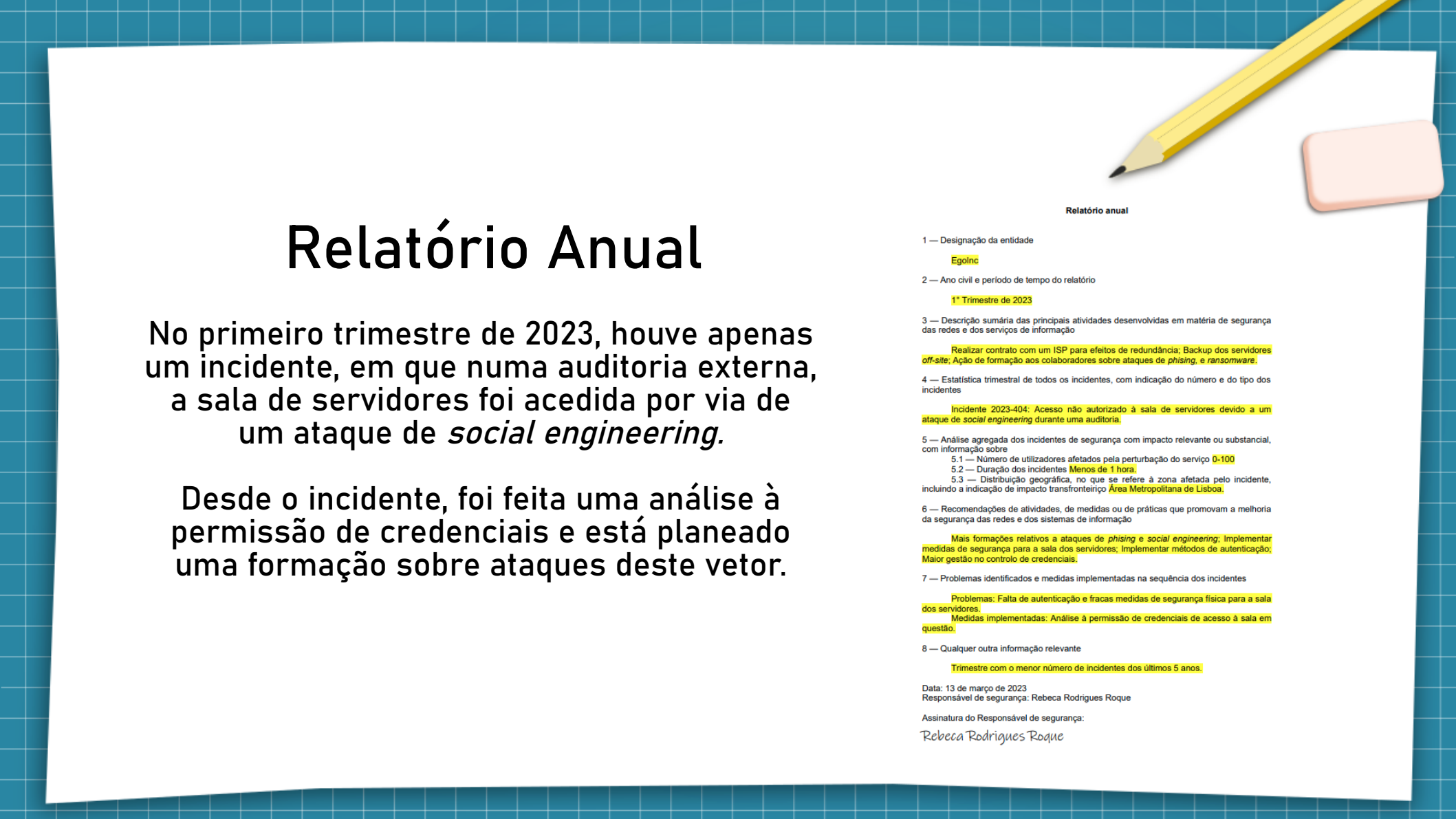
Lista de ativos

Serviço Suportado	Nome do equipamento/software	Modelo/Versão	Endereço IP (se aplicável)	FQDN (se aplicável)	Fabricante
Servidor 1	Rocky Linux	ThinkSystem SR665 (AMD EPYC 7252, 512GB RAM)	10.10.10.1	rocky.ego.inc	Lenovo
Servidor 2	Windows Server 2003	ThinkSystem SR665 (AMD EPYC 7252, 512GB RAM)	10.10.10.2	win.ego.inc	Lenovo
Router	UniFi	UniFi Dream Machine Pro 8TB	10.10.10.254	dream.ego.inc	Ubiquiti
Switch	UniFi	Switch Pro 48 PoE	N/A	N/A	Ubiquiti
Firewall	pfSense+	Netgate 1537 pfSense+ Security Gateway	10.10.10.253	sense.ego.inc	Netgate

Relatório Anual

No primeiro trimestre de 2023, houve apenas um incidente, em que numa auditoria externa, a sala de servidores foi acedida por via de um ataque de *social engineering.*

Desde o incidente, foi feita uma análise à permissão de credenciais e está planeado uma formação sobre ataques deste vetor.



Relatório anual

1 — Designação da entidade

EgoInc

2 — Ano civil e período de tempo do relatório

1º Trimestre de 2023

3 — Descrição sumária das principais atividades desenvolvidas em matéria de segurança das redes e dos serviços de informação

Realizar contrato com um ISP para efeitos de redundância; Backup dos servidores *off-site*; Ação de formação aos colaboradores sobre ataques de *phising*, e *ransomware*.

4 — Estatística trimestral de todos os incidentes, com indicação do número e do tipo dos incidentes

Incidente 2023-404: Acesso não autorizado à sala de servidores devido a um ataque de *social engineering* durante uma auditoria.

5 — Análise agregada dos incidentes de segurança com impacto relevante ou substancial, com informação sobre

5.1 — Número de utilizadores afetados pela perturbação do serviço 0-100

5.2 — Duração dos incidentes Menos de 1 hora.

5.3 — Distribuição geográfica, no que se refere à zona afetada pelo incidente, incluindo a indicação de impacto transfronteiriço Área Metropolitana de Lisboa.

6 — Recomendações de atividades, de medidas ou de práticas que promovam a melhoria da segurança das redes e dos sistemas de informação

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

7 — Problemas identificados e medidas implementadas na sequência dos incidentes

Problemas: Falta de autenticação e fracas medidas de segurança física para a sala dos servidores.

Medidas implementadas: Análise à permissão de credenciais de acesso à sala em questão.

8 — Qualquer outra informação relevante

Trimestre com o menor número de incidentes dos últimos 5 anos.

Data: 13 de março de 2023
Responsável de segurança: Rebeca Rodrigues Roque

Assinatura do Responsável de segurança:

Rebeca Rodrigues Roque

Perguntas?