

Levantamentos, avaliações e resultados na Universidade de Évora

Joaquim Godinho
Direcção de Serviços de Informática

Patrocinadores Platina



Patrocinadores Ouro



Patrocinadores Prata



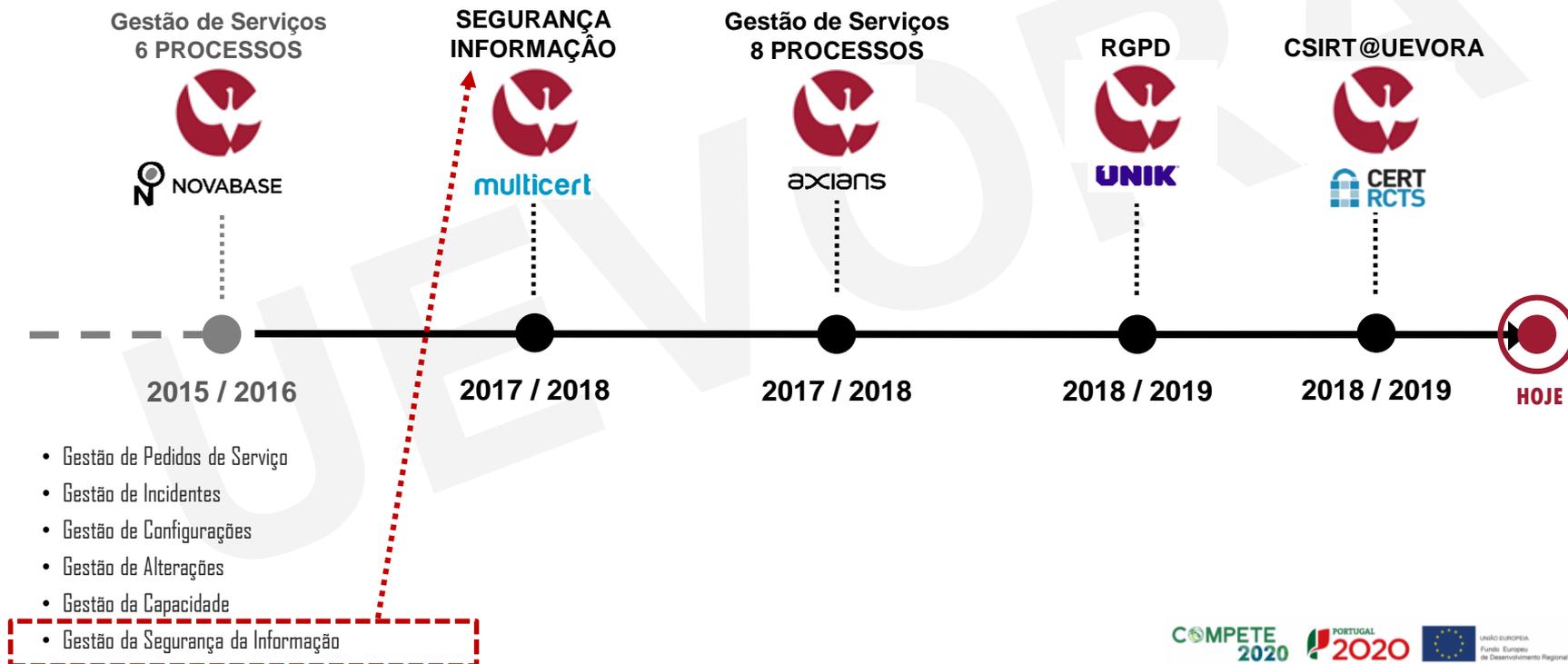
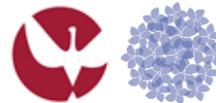
Apoios



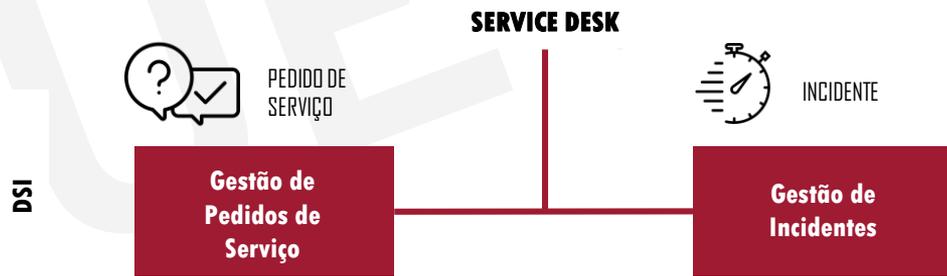
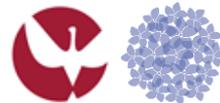
Organização



A História...



Visão Geral do Sistema de Gestão de Serviços TI



MODELO DE GESTÃO DE SERVIÇOS



Processo de Gestão de Incidentes e Pedidos de Serviço



Restaurar o serviço e executar pedidos de serviço, dentro dos níveis de serviço acordados.

Incidentes / Incidentes Graves

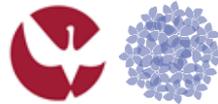


Pedidos de Serviço



O QUE EU VOU CONSEGUIR COM ESTE PROCESSO ?

- 1** Controlo sobre todo o ciclo de vida dos incidentes e pedidos de serviço reportados (desde o seu registo ao seu fecho).
- 2** Incidentes e pedidos de serviço registados, classificados, priorizados, analisados, resolvidos e fechados.
- 3** Informação rápida sobre o estado e o progresso de resolução dos incidentes e pedidos de serviço reportados.
- 4** Visibilidade sobre os incidentes e pedidos de serviço não resolvidos de acordo com os níveis de acordo de serviço (SLA) definidos.
- 5** Partilha de informação relevante para a correção e resolução de incidentes e pedidos de serviço entre as equipas de trabalho.
- 6** Maior eficiência e produtividade na correção e resolução de incidentes e pedidos de serviço entre as equipas de trabalho.



Gestores de incidentes são os “super-heróis” do ITIL e o seu lema é “resolver depressa !”



INCIDENTE

- Os incidentes são interrupções de um serviço, uma redução na qualidade desse serviço ou uma falha de um componente.
- São eventos inesperados e não planeados que devem ser tratados com a maior brevidade possível e são, juntamente com os pedidos de serviço a principal responsabilidade de um *ServiceDesk*.
- Um incidente (ou mais) pode originar o registo de um problema.
- Os incidentes precisam ser registados na aplicação do *ServiceDesk* para que possam ser monitorizados e rastreados.

PROBLEMA

- Os problemas são o PORQUÊ / a causa raiz de um ou mais incidentes.
- Corrigir um problema geralmente requer testes para descobrir qual é a causa que lhe está subjacente e deste modo encontrar uma solução permanente.

Gestores de problemas são os “investigadores do CSI” que investigam as causas, colocam as questões adequadas, identificam o que aconteceu, porquê e como resolver de forma definitiva.



Processo de Segurança da Informação



Gerir a segurança da informação ao nível acordado, dentro de todas as atividades de gestão de serviços

Segurança da Informação



O QUE EU VOU CONSEGUIR COM ESTE PROCESSO ?

* **Controlos:** Meios de gerir o risco, que inclui políticas, procedimentos, linhas de orientação, práticas ou estruturas organizacionais. O risco pode ser de natureza administrativa, tecnológica, de gestão ou legal.



**Política de Segurança da Informação
+ Segurança Física e Ambiental
+ Segurança das Comunicações
+ Segurança das Operações**

Âmbito:
**Serviços de
Informática**

Gestão de Risco

Conselho/Equipa de Segurança da Informação

Relatório de Avaliação do Risco de Segurança da Informação



Abordagem sistemática para uma gestão de riscos de segurança da informação mais eficaz e eficiente.



Aumento da fiabilidade e segurança da informação (no seus vários formatos) e dos sistemas, em termos de confidencialidade, integridade e disponibilidade.



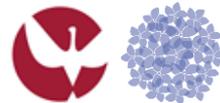
Criação de uma cultura de segurança da informação, com o entendimento dos riscos e adoção de controlos como parte das práticas diárias de trabalho da organização.



Redução dos custos e alocação de recursos, com a implementação de controlos apropriados e suficientes.

Open-source Ticket Request System (OTRS)

Solução de gestão de serviços



- **ServiceDesk**
- **Gestão de Incidentes e Pedidos de Serviço**
- **Gestão de Alterações**
- **CMDB (integrada com o Sistema de Informação da Universidade)**

... Incidentes de Segurança



... MAIOR TRANSPARÊNCIA

O OTRS permite a customização do catálogo de serviços, de acordo com as necessidades de serviços e infraestrutura da Organização.



... FÁCIL INTEGRAÇÃO

O OTRS permite a integração com outras soluções como o NAGIOS e OCS.



... RESPOSTAS RÁPIDAS

A automatização de processos e a integração de ferramentas de gestão de conhecimento permitem resultados rápidos e de alta qualidade.



... SUPORTE AOS UTILIZADORES

O OTRS permite aos utilizadores categorizarem e descreverem os incidentes e os pedidos de serviço, de forma fácil, rápida e segura.



... SIMPLIFICAÇÃO DA GESTÃO DE TICKETS

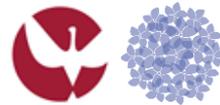
O OTRS permite a criação de filas de trabalho que recebem de forma automática a informação necessária para efetuarem a sua gestão de tarefas e prioridades.



... ESTATÍSTICAS E RELATÓRIOS

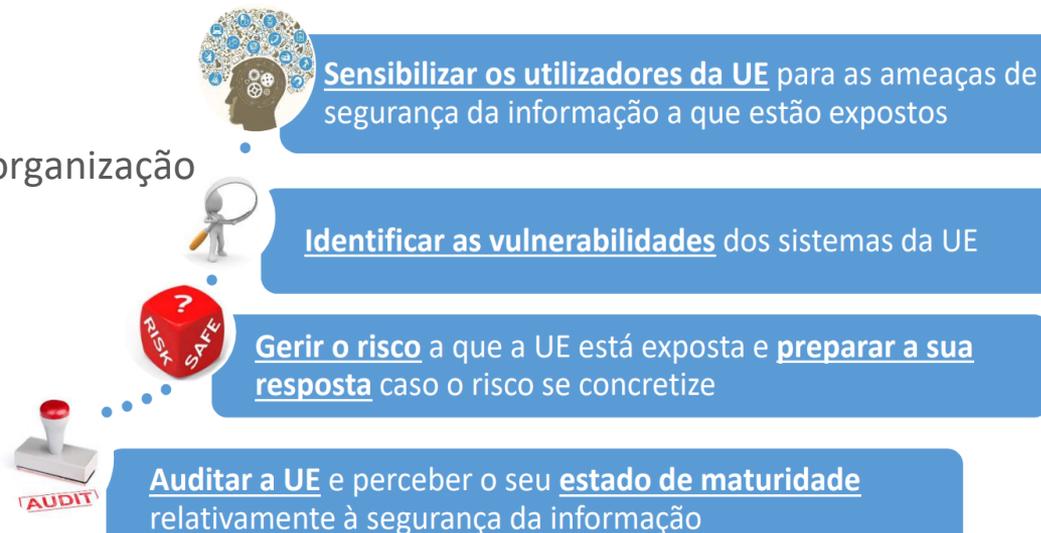
O OTRS permite a recolha de estatísticas e relatórios dinâmicos que vão suportar e facilitar a tomada de decisões.

Segurança da Informação (2017/18)



- Avaliação de *awareness* em Segurança da Informação
 - Realização de inquérito dirigido a todos os colaboradores da Universidade
- Sensibilização para a Segurança da Informação
 - Realização de workshop dirigido a responsáveis e “utilizadores-chave”
- Realização de Testes de Intrusão
 - Infraestruturas e serviços
- Divulgação e sensibilização a toda a organização
 - Comprometimento da gestão

Âmbito:
Universidade,
Serviços de
Informática
e
Serviços
Académicos



Segurança da Informação...o que falta fazer!

Âmbito do Projeto
mSecurity@UnivEvora

Funções e Responsabilidades

Identifica funções e responsabilidades na SI

Controlo de Acessos

Gere os controlos de acessos lógicos

Aquisição, Desenvolvimento e Manutenção de Sistemas

Gestão informática dos sistemas

Gestão da Mudança

Identifica como é gerida a mudança (organizacional e nos sistemas)

Gestão do Risco

Gere o risco da organização e recursos

Segurança Física

Gere as instalações físicas e controlos de segurança associados

Gestão Operacional

Gestão da mudança informática dos sistemas

Gestão da Mudança

Gere a capacidade dos recursos (atual e futura)

Gestão da Continuidade de Negócio

Prepara a organização para reagir a interrupções de negócios

Gestão de Recursos/Ativos

Gere o inventário de recursos

Gestão de Comunicações

Gere a segurança da informação nas redes

Gestão de Incidentes de Segurança da Informação

Identifica a forma como são geridos e resolvidos os incidentes

Gestão de Recursos Humanos

Gere a política, permanência e saída de colaboradores incluindo formação

Gestão de Documentos

Gestão documental (documentos físicos e digitais)

Criptografia

Define os controlos criptográficos utilizados

Gestão de Auditorias

Define as auditorias a realizar, passos executados e prazos

Gestão de Fornecedores

Gere a relação com os fornecedores (contratos e cláusulas associadas, etc)

Classificação de Informação

Define os níveis de classificação de informação e requisitos associados

Utilização Aceitável de Internet

Define práticas permitidas e proibidas na utilização da internet

Conformidade

Gere a identificação de nova legislação/conformidade a sua implementação



7.1 BILIÕES DE IDENTIDADES FORAM EXPOSTAS DEVIDO A FALHAS DE SEGURANÇA, NOS ÚLTIMOS 8 ANOS. NÃO VAMOS AUMENTAR ESSE NÚMERO!

SIGA AS BOAS PRÁTICAS DE SEGURANÇA DE INFORMAÇÃO



Gestão de Palavras-Passe Mantenha-as seguras!

As palavras-passe são utilizadas como forma de autenticação e proteção. São elas que separam os atacantes da sua informação sensível.



DICAS

Utilize passphrases ao invés de palavras-passe, por exemplo: "sozinhos vamos mais rápido juntos vamos mais longe", ou se existir um limite de caracteres, por exemplo "eu nasci em evora no ano de 1559" = eN@ENAd59

Utilize gestores de palavras-passe - que guardem as suas palavras-passe em modo cifrado, para que não necessite de as memorizar. Dê preferência a gestores que funcionem localmente em detrimento de Serviços que guardam as palavra-passe na Cloud.

Altere a palavra-passe através do SIUE - utilize este sistema de palavras-passe que utiliza no acesso aos serviços/sistemas da Universidade

Não reutilize as suas palavras-passe, nem utilize a mesma palavra-passe em contexto pessoal e profissional - se o seu e-mail é utilizado no âmbito pessoal for comprometido, não irá colocar em risco os serviços que utiliza no âmbito profissional.

Apps São seguras?

Milhões de apps são feitos diariamente para os dispositivos móveis. Não desconfie de apps desconhecidas. E mesmo que sejam de app stores oficiais podem não ser 100% seguros!



DICAS

Utilize o seu sistema operativo sempre se fosse o seu computador - Com os mesmos cuidados que utiliza no seu sistema operativo, browser, antivírus, firewall e apps atualizados!

Não instale apps fora das app stores oficiais - Utilize sempre fontes oficiais.

Não instale apps que não utiliza - Especialmente quando necessitam de permissões para aceder ao microfone, câmara, localização ou ficheiros do seu dispositivo. Reduza este tipo de permissões ao mínimo!

Antivírus e Atualização do sistema operativo e browser Proteja-se do malware!

Frequentemente são identificadas vulnerabilidades no sistema operativo e/ou browser que utiliza, colocando em causa a segurança de informação. Atualize o sistema operativo, browser ou antivírus para não estar vulnerável a fraquezas conhecidas pelos atacantes.



DICAS

Garanta que tem o seu sistema operativo e browser atualizado - Instale atualizações automáticas para o seu sistema operativo e browser. Assim, estará protegido contra vulnerabilidades conhecidas.

Phishing* seja apanhado!

Phishing é uma técnica utilizada por criminosos para obter dados pessoais e financeiros através de e-mails, mensagens de texto ou redes sociais. Os atacantes tentam parecer com entidades conhecidas para obter dados pessoais e financeiros através de e-mails, mensagens de texto ou redes sociais.

*São emails fraudulentos que procuram atrair a atenção dos utilizadores com remetentes forjados ou com assuntos suspeitos, para obter dados sensíveis ou fazê-lo visitar sites maliciosos.

DICAS

Verifique se o email é fidedigno - Se o remetente corresponde ao nome que aparece, não existem erros ortográficos que chamem a atenção e tente validar o remetente através de outros meios de comunicação, por exemplo por telefone.

Atenção aos emails fraudulentos! - Evite abrir emails e anexos de remetentes desconhecidos e verifique os links antes de clicar, passando o rato por cima (mouse over). Apague o email de imediato!

Não envie dados sensíveis (palavras-passe, moradas, dados bancários, dados pessoais) por email. - Mesmo que não tenham acesso ao seu dispositivo, poderão conseguir interceptar a informação.

Financiado por:



Acesso seguro à Internet

Recursos disponíveis

Todos os dias se conectamos à internet. Muitas vezes utilizamos redes Wi-Fi para termos acesso à internet. No entanto, a informação que transmitimos e os seus dispositivos podem ser capturados e utilizados por terceiros para serem infectados.



Utilize o certificado digital para configurar o acesso Wi Fi à rede eduoram. Garanta a segurança das comunicações. Mais informação disponível em <http://wifi.uevora.pt/>

Evite aceder a websites que não sejam HTTPS - Verifique sempre que o website que pretende aceder tem o cadeado verde e a ligação é cifrada (<https://>)

Evite transações de elevado risco em redes wireless públicas - Não aceda à sua conta bancária online ou aos serviços da universidade que contenham informação sensível. Em alternativa, utilize para esse efeito a rede do seu dispositivo móvel e mantenha-o sempre atualizado.

Não confie no nome da rede wireless, pode ser falsa - Garanta que está a usar uma rede fidedigna no local certo (por exemplo, só poderá conectar-se à rede wireless de sua casa se estiver em casa).

Clean Desk / Clear Screen what you see is what you get!

Todos os dias manuseamos informação em papel que depositamos em cima da mesa. Trabalhamos informação digital nos dispositivos e saímos de perto deles sem os bloquear. Para o atacante se houver informação visível pode tornar-se apetecível!

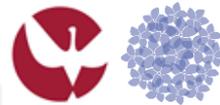


DICAS

Mantenha a sua informação segura - Bloquee o equipamento na sua ausência. Configure sempre dispositivos de bloqueio automático no seu computador, portátil e smartphone (password, PIN, padrão, etc)

Não deixe documentos em cima da mesa - Principalmente se contiverem informação sensível/pessoal. Guarde a documentação num local seguro.

Regulamento Geral de Proteção de Dados (2018/19)



Tipo	Data ▲	Assunto
Ordem de serviço	2018-03-15	Regulamento do Conselho de Segurança da Informação e Proteção de Dados Pessoais da Universidade de Évora
Despacho	2018-05-09	Regulamento do Conselho de Segurança da Informação e Proteção de Dados Pessoais
Despacho	2018-05-24	Nomeação do Encarregado de Proteção de Dados da Universidade de Évora
Despacho	2018-06-06	Composição do Conselho de Segurança da Informação e Proteção de Dados Pessoais

Artigo 3º Composição

- O CSIPDP é composto pelos seguintes membros:
 - Presidente, cargo exercido pelo Reitor, ou titular com competências delegadas;
 - Encarregado da Proteção de Dados (EPD);
 - Responsável pela Segurança de Informação (RSI);
 - Um representante de cada Unidade Orgânica;
 - O Administrador da Universidade de Évora.
- Os membros referidos nas alíneas b) a c) são designados pelo Reitor.

Adenda : f) Director dos Serviços de Ação Social

Artigo 5º

Encarregado da Proteção de Dados

- O encarregado da proteção de dados tem as competências e funções definidas para o “Encarregado da Proteção de Dados” (*Data Protection Officer*), no âmbito do Regulamento Geral de Proteção de Dados.

Artigo 6º

Responsável pela Segurança de informação

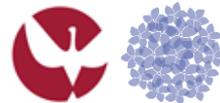
- O Responsável pela Segurança de Informação (*Chief Information Security Officer*) é a pessoa responsável pela coordenação e implementação da Gestão de Segurança da Informação na Universidade.
- O Responsável pela Segurança de Informação reporta ao Reitor para garantir a disponibilidade dos recursos necessários, para a operacionalização e melhoria contínua da Gestão de Segurança da Informação.

Regulamento Geral de Proteção de Dados (2018/19)



- Ambiente académico, dinâmico e pouco regulado
- Autonomia na...
capacidade de decisão e ... de implementação
(UE = Data controller + Data processor)
- “Cultura organizacional fragmentada”
- Muuuitoos dados pessoais: alunos, colaboradores, fornecedores, parceiros...
- Adotar uma abordagem incremental e modular
 - por áreas: académica, científica, administrativa...
 - por unidades: Escolas, Serviços,...
 - por domínios: legal, procedimental e técnico
- Assegurar apoio externo especializado
- Adquirir e reforçar competências internas : formação + sensibilização
- Promover uma “cultura” adequada : bom senso e ética + compromisso

Regulamento Geral de Proteção de Dados (2018/19)



- Avaliação de conformidade com o RGPD;
- Identificação dos dados pessoais e dados pessoais sensíveis, categorias e formas de tratamento;
- Elaboração de um Plano de Implementação do RGPD;
- Sensibilização dos “stakeholders”, dos responsáveis e dos utilizadores em geral relativamente ao RGPD



CSIRT.UEVORA

Introdução

Com a contínua expansão da Internet e o seu uso crescente por serviços críticos, a estabilidade e disponibilidade destes torna-se cada vez mais importante. Incidentes como quebras de serviço, roubo ou vandalismo podem ter consequências graves em termos financeiros, de reputação e com consequências legais.

Sempre que há um incidente de cibersegurança, uma resposta rápida e eficaz é fundamental. Para tal, foi criado o CSIRT.UEVORA.

Quem somos

O CSIRT.UEVORA (Computer Security Incident Response Team) é uma entidade da Universidade de Évora, composta por especialistas em informática. É constituída por especialistas em segurança informática e capacidade para identificar e responder a incidentes.

Missão

Compete ao CSIRT.UEVORA dar uma primeira e rápida resposta a incidentes de segurança na Universidade de Évora, focando-se na salvaguarda da informação contida nos seus sistemas de informação bem como agir para mitigar eventuais falhas identificadas.

Procura também, proactivamente, identificar riscos e vulnerabilidades nos sistemas informáticos da Universidade de Évora e fomentar boas práticas de segurança da informação na comunidade académica.

2013' Criação do e-mail csirt@uevora.pt

2018' Criação do csirt.uevora; adesão à RAC

- **Formalização interna. despacho reitoral**
- **Divulgação à comunidade**
- **Articulação com outras iniciativas no domínio da segurança e proteção de dados**

- 97 incidentes registados desde 2013 (Sem contar com violação de copyright)
- 7 em 2019 (ate Abril)
 - Páginas comprometidas
 - Contas comprometidas
 - Serviços inseguros, Spamming, Brute force...
- Nem todos foram registados...
- Alertas RCTS-CERT

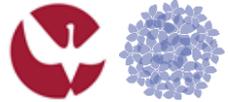
Incidente de Segurança

Registo CSIRT@UEVORA:

> OTRS “Checked”

Atribuição de responsável

Registo de resolução



Ticket#2019011874000783 — Bruteforce nos wordpresses do janus

Dashboard Customers Calendar Tickets FAQ Services CMDB ITSM Changes Survey Reports Admin

Back | Print | Priority | People | Communication | Pending | Watch | Close | Miscellaneous | Queue

Article Overview - 3 Article(s)

NO.	SENDER	VIA	SUBJECT	DATE
3	Tiago Sousa	OTRS	Bruteforce nos wordpresses do janus	01/18/2019 17:42
2	Tiago Sousa	OTRS	Bruteforce nos wordpresses do janus	01/18/2019 17:42
1	Tiago Sousa	Phone	Bruteforce nos wordpresses do janus	01/18/2019 17:42

#3 – suricata + fail2ban – Tiago Sousa – 01/24/2019 18:13 via OTRS by Tiago Sousa

Reply to note | Mark as read | Split

...a possibilidade de usar o fail2ban no mundo para bloquear com o arquivo /var/log/suricata/suricata.log.

#2 – Falhou marcar o incidente de segurança – Tiago Sousa – 01/18/2019 18:13 via OTRS by Tiago Sousa

Reply to note | Mark as read | Split

... Bruteforce nos wordpresses do janus – Tiago Sousa – 01/18/2019 17:42 via Phone by Tiago Sousa

Mark | Print | Split | Forward | Reply

Esta tarde o servidor janus acusou um pico de carga fora do normal. Foi investigar e pelo server-status do apache percebia-se que tinha uma grande carga causada por acessos ao wp-login.php, a página de login do wordpress. Numa primeira abordagem tentei banir alguns ips manualmente mas percebi que era inefetivo, os acessos vinham de IPs sempre diferentes.

A solução foi usar o fail2ban para analisar o access.log de todos os vhosts e banir os IPs que acedam repetidamente a este ficheiro. Não precisamos de saber se o login teve sucesso ou não, pois podemos deprender que se for necessário aceder várias vezes é porque o login não se concretizou.

Criei uma regra genérica com base em sugestões online, mas depois aperfeiçoei a regra para ser mais rígida quando o acesso tem o user-agent "python-requests". Neste momento baneu um dia inteiro com apenas 2 acessos desse user agent. Já estão banidos 1400 IPs e continua a subir. Um ponto importante é o fail2ban do servidor não suportar IPv6, pelo que tive de fazer alguns bloqueios manuais "agressivos" a /16 e /32, mas parece ter resultado para já.

Algo a ter em conta para outras páginas e servidores, e replicar! Além disso, numa estratégia de segurança integrada do SIEM, estes IPs deveriam ser banidos na firewall central. O próprio suricata deve conseguir fazer este trabalho desde que os acessos sejam por http, coisa que até tem acontecido, mas deveria haver outros métodos de organização e sincronização.

Ticket Information

Type: Incidentes
Age: 108 d 3 h
Created: 01/18/2019 17:42
Created by: Tiago Sousa
Created by phone number: 912345678
Lock: Locked
Queue: Infraestruturas e Serviços
Service: Alojamento Web
Service Incident: Operational
State: Open
Service Level: Incidentes - Prioridade
Agreement: Média - Resolução
Criticality: 2 medium
Impact: 3 high urgency
Priority: 2 medium
Customer ID: mirage@uevora.pt
Accounted time: 0

Owner: Tiago Sousa
Responsible: Tiago Sousa

Incidente de Segurança: Checked

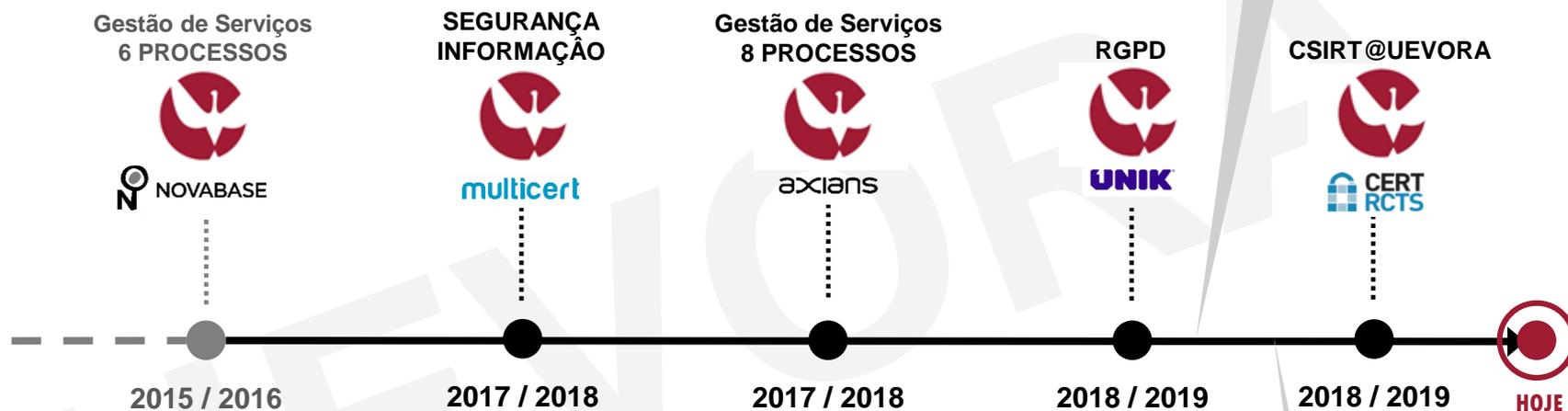
Customer Information

Firstname: Tiago
Lastname: Sousa
Username: mirage
Email: mirage@uevora.pt
Open tickets (customer) (1)

Moral da história...

O que correu bem

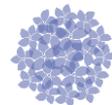
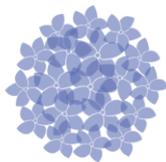
- Fases de “formação e sensibilização” e “apoio à implementação” cruciais para o desenvolvimento do projeto
- Evolução notória do nível de maturidade
- Demonstração das competências e capacidade da equipa



- **Colaboração “inter-pares” e Competências Internas vs**
- **Apoio Externo**
- **Mudança de mentalidade/cultura em toda a “organização”**
- **Disponibilidade de recursos (financeiros, humanos, materiais)**

O que podia ter corrido melhor

- Comunicação e gestão das expectativas da equipa ao longo do projeto
- “Sponsorship” da gestão de topo
- Mobilização da “comunidade”



Obrigado

jjg@uevora.pt

Patrocinadores Platina



Patrocinadores Ouro



Patrocinadores Prata



Apoios



Organização

