Ciclo de desenvolvimento seguro:

Pessoas, Processos e ferramentas.

Gustavo Lichti Mendonça

{ Geru }

GERU

- **[Temos vagas!]**

- **[Respeitamos as diferenças!]**

GERU

Porque falar em desenvolvimento seguro ???

{ Vazamentos }

Economia

Uber começa a notificar brasile vazam

12 abr 201

Economia

Netshoes avisará clientes por telef vazamer

27 fev 2018, 13

Economia

Banco Inter confirma vazamer clientes

17 ago 2018, 0

Verizon vai comprar Yahoo mais barat ciberataque

Convergência Digital ... 21/

A operadora american 21/2, que vai pagar me passado por US$ 4,83 'desconto' de quase R ciberataques admitido

Novo ataque põe em xeque venda do Yahoo!

Verizon ameaça abandonar acordo de US$ 4,8 bi por temor de processos envolvendo dados roubados por hackers

Redução do valor também estaria sendo estudada por grupo de telefonia, que teme fuga em massa de usuários

"FINANCIAL TIMES"

A oferta de US$ 4,8 bilhões da Verizon pela compra do Yahoo! corre o risco de desabar depois que a gigante de tecnologia revelou um ataque cibernético afetando mais de 1 bilhão de contas de seus usuários em todo o planeta.

A admissão de que dados pessoais de usuários foram roubados em 2013 surgiu apenas meses depois que uma investigação separada constatar que mais de 500 milhões de contas do Yahoo! haviam sido invadidas em 2014.

O Yahoo! revelou o vazamento de dados de 2014 em setembro, apenas dois meses após fechar acordo com a Verizon para a venda à empresa de telefonia de suas principais operações de internet.

Uma equipe de advogados da Verizon está trabalhando para decidir se é possível salvar a transação sem expor a companhia americana de telefonia a futuros processos associados aos dados roubados pelos hackers, disseram duas pessoas próximas aos gestores da companhia.

As fontes disseram que a empresa será forçada a abandonar o acordo ou buscar uma redução no preço negociado, a menos que a Verizon consiga construir uma barreira que a proteja contra futuros problemas legais relacionados à violação da privacidade de dados.

O Yahoo! disse que ainda não sabe de que forma os hackers haviam obtido os dados roubados em 2013.

Um porta-voz do Yahoo! disse confia confir à inte Em mo, v zon, d são às "uma te gra po de va tra ção d to ma A V a pos sumid hool

depois das duas imensas ex- sa estratégia, disse a fonte.

Marriott Announces Starwood Guest Reservation Database Security Incident

By PR Newswire, November 30, 2018, 06:00:00 AM EDT

{ 2019... }

GERU

Falha no Twitter expôs contas e tweets privados no Android desde 2014

POR **DOUGLAS CIRIACO** | @dciriaco - EM **REDES SOCIAIS** - 18 JAN 2019 — 11H39

Dados de 1,4 milhão de clientes do Banco Inter estavam expostos para acesso

POR **FELIPE PAYÃO** | @felipepayao - EM **SEGURANÇA** - 13 FEV 2019 — 15H48

Vazam dados sensíveis de 40 mil clientes da Taurus Armas

POR **FELIPE PAYÃO** | @felipepayao - EM **SEGURANÇA** - 14 FEV 2019 — 15H59

O que o Gartner e a estatística dizem sobre ataques cibernéticos ?

O que o Gartner e a estatística dizem sobre ataques cibernéticos ?

8 em 10 ataques visam a camada de aplicação

Como reduzir o risco e aumentar a segurança ?

GERU

Como reduzir o risco e aumentar a segurança ?

DevSecOps

{ Mas o que é DevSecOps ? }

GERU

[RedHat]

DevSecOps significa pensar em segurança de aplicativos e infraestrutura desde o início

GERU

[Como fazer funcionar?]

Pessoas

Processos

Ferramentas

[Como fazer funcionar?]

Pessoas

[Cultura / Treinamentos]

- Alinhamento;
- Conscientização;
- Treinamento;
- Exemplo;
- Prática.

GERU

[Como fazer funcionar?]

Pessoas

Processos

[Medição / Qualidade]

- Code review;
- Guidelines;
- Métricas;
- Monitoramento;
- Compliances.

[Guidelines]

- MS SDL;
  - Security Development Lifecycle;
- NIST 800-64;
  - Security Considerations in the System Development Life Cycle;
- OWASP SAMM;
  - SOFTWARE ASSURANCE MATURITY MODEL.

{ Processos }

[Code review]

- Code Review no PR para staging;
- “First review” automatizado;
- Review por outros devs;
- Review por um tech lead;
- OWASP Code Review Guide.

{ Processos }

[Compliances]

- LGPD;
- GDPR;
- Bacen 4658/2018;
  - Privacy by design;
  - Security by default.

GERU

[Como fazer funcionar?]

Pessoas

Processos

Ferramentas

{ Ferramentas }

GERU

[WAF]

- OWASP ModSecurity.

[SQL]

- Sqlmap.

[Code Smells]

- SonarQube.

{ Ferramentas }

GERU

[Vulnerabilidades]

- OWASP ZAP;
- W3af.

[Containers]

- Clair;
- Docker Bench Security.

[Dependencias]

- OWASP Dependency-Check.

{ Ferramentas }

[SAST]

- Bandit (Python);
- Brakeman (Ruby);
- Google CodeSearchDiggity (SQLi, XSS);
- SonarQube (20 languages for Bugs, Vulnerabilities, and Code Smells).

[CI/CD]

- Jenkins.

{ Ferramentas }

[Configuration Management]

- Ansible;
- Puppet;
- Chef.

[Secrets Management]

- Vault;
- Conjur.

{ Ferramentas }

[Infra-as-a-Code]

- Terraform;
- Ansible.

{ Ferramentas }

[OpenSource]

- 1 > 0;
- Custo;
- Aprendizado;
- OWASP.

Não existe software 100% seguro

GERU

Não existe software 100% seguro

O que fazer ?

GERU

Não existe software 100% seguro

Automação!

{ Não existe software 100% seguro }

[O que fazer ?]

- Monitorar;
- Saber responder a incidentes;
- Red Team / Blue Team;
- Bug bunty.

{ Obrigado }

GERU

/gustavo-lichti

/gustavo_lichti

/gustavo.lichti

/lichti

/lichti

www.lichti.com.br

gustavo.lichti@gmail.com

/company/geru

/geru_br

/GeruBrasil

/geru_br

/geru-br

www.geru.com.br

{ Geru }

GERU

- **[Temos vagas!]**

- **[Respeitamos as diferenças!]**