PCI Data Security Standard

Luiz Gustavo C. Barbato

gbarbato@trustwave.com

GTS 11 – 01/06/2008

O que é um Comprometimento de Cartão de Crédito?

Conseguir acesso não autorizado através de alguma vulnerabilidade em ambientes que:

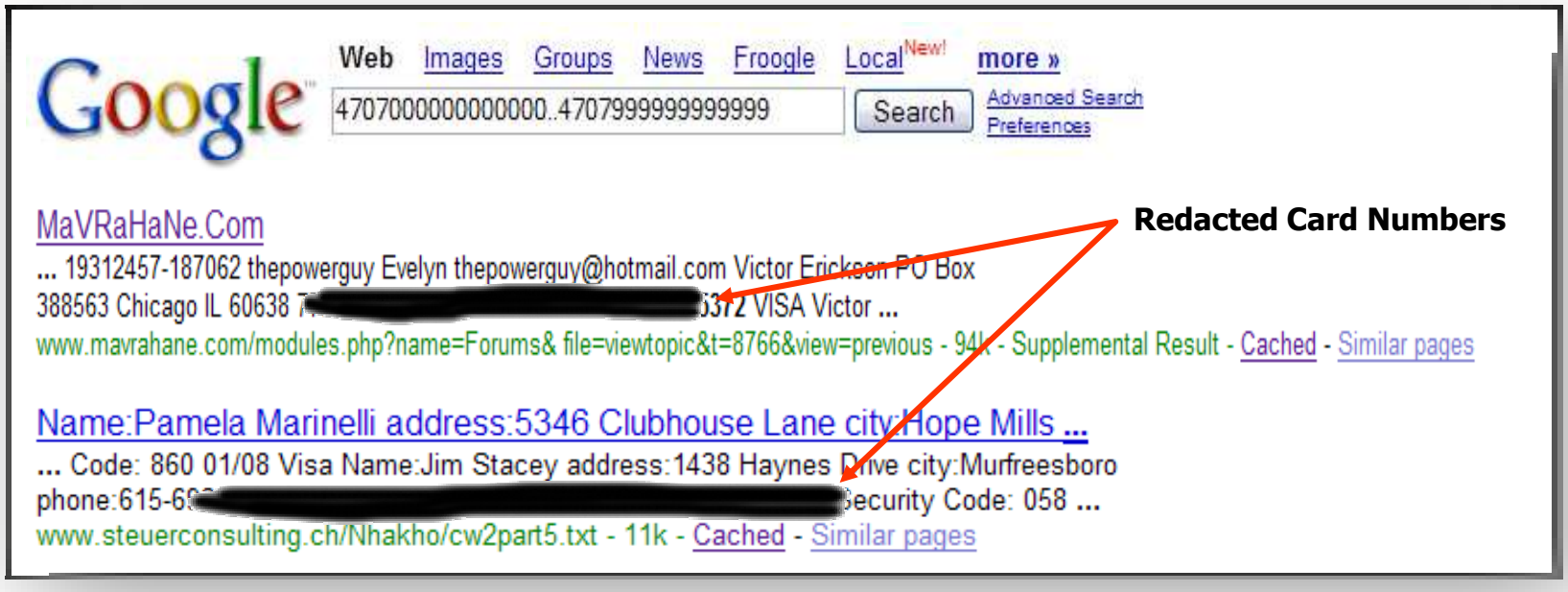
Processam, transmitem ou armazenam os dados do portador do cartão

Para ter acesso a:

- Números de Cartões (PAN)
- Datas de expiração
- Códigos de Segurança (CVV2/CVC2/CID)
- Dados da Trilha

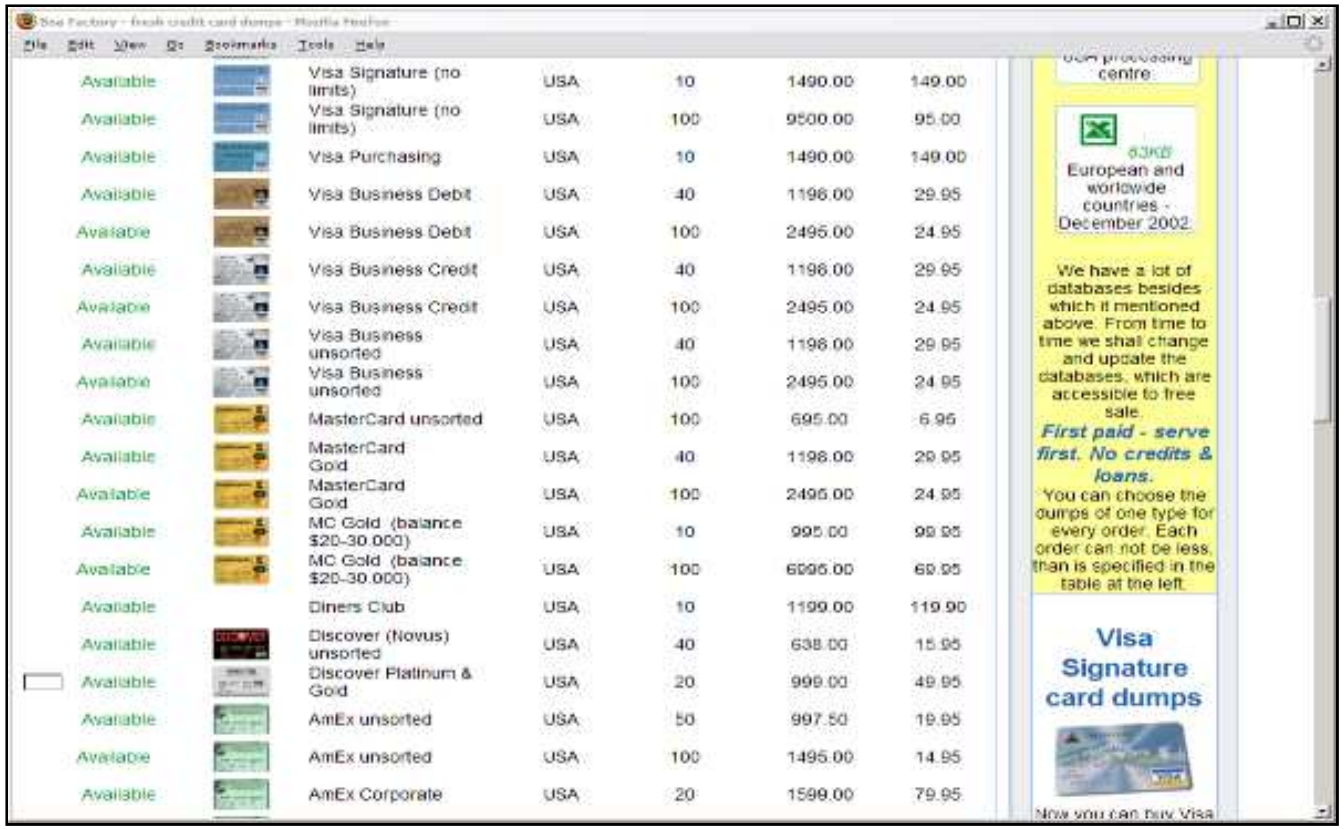
… e é Mais Fácil que Muitos Pensam

- Números de cartões comprometidos foram encontrados em *websites* públicos



Venda de Dados de Cartão é Lucrativa

- Uma vez comprometidos…



Available		Visa Signature (no limits)	USA	10	1490.00	149.00
Available		Visa Signature (no limits)	USA	100	9500.00	95.00
Available		Visa Purchasing	USA	10	1490.00	149.00
Available		Visa Business Debit	USA	40	1196.00	29.95
Available		Visa Business Debit	USA	100	2495.00	24.95
Available		Visa Business Credit	USA	40	1196.00	29.95
Available		Visa Business Credit	USA	100	2495.00	24.95
Available		Visa Business unsorted	USA	40	1196.00	29.95
Available		Visa Business unsorted	USA	100	2495.00	24.95
Available		MasterCard unsorted	USA	100	695.00	6.95
Available		MasterCard Gold	USA	40	1196.00	29.95
Available		MasterCard Gold	USA	100	2495.00	24.95
Available		MC Gold (balance $20-30.000)	USA	10	995.00	99.95
Available		MC Gold (balance $20-30.000)	USA	100	6995.00	69.95
Available		Diners Club	USA	10	1199.00	119.90
Available		Discover (Novus) unsorted	USA	40	638.00	15.95
Available		Discover Platinum & Gold	USA	20	999.00	49.95
Available		AmEx unsorted	USA	50	997.50	19.95
Available		AmEx unsorted	USA	100	1495.00	14.95
Available		AmEx Corporate	USA	20	1599.00	79.95

centre

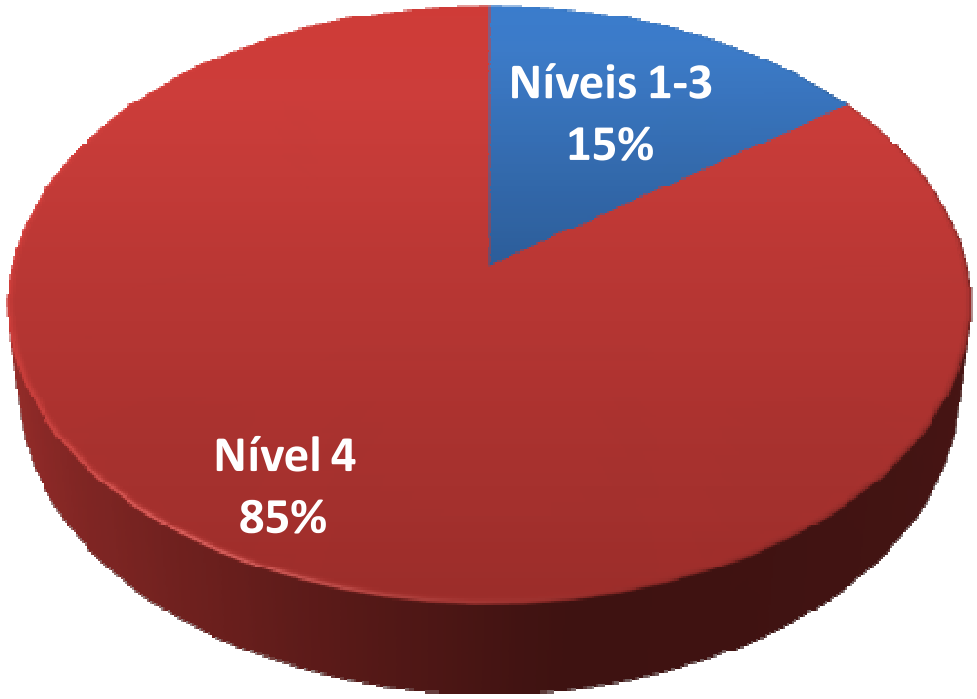
63KB
European and worlowide countries - December 2002

We have a lot of databases besides which it mentioned above. From time to time we shall change and update the databases, which are accessible to free sale.
First paid - serve first. No credits & loans.
You can choose the dumps of one type for every order. Each order can not be less, than is specified in the table at the left.

Visa Signature card dumps

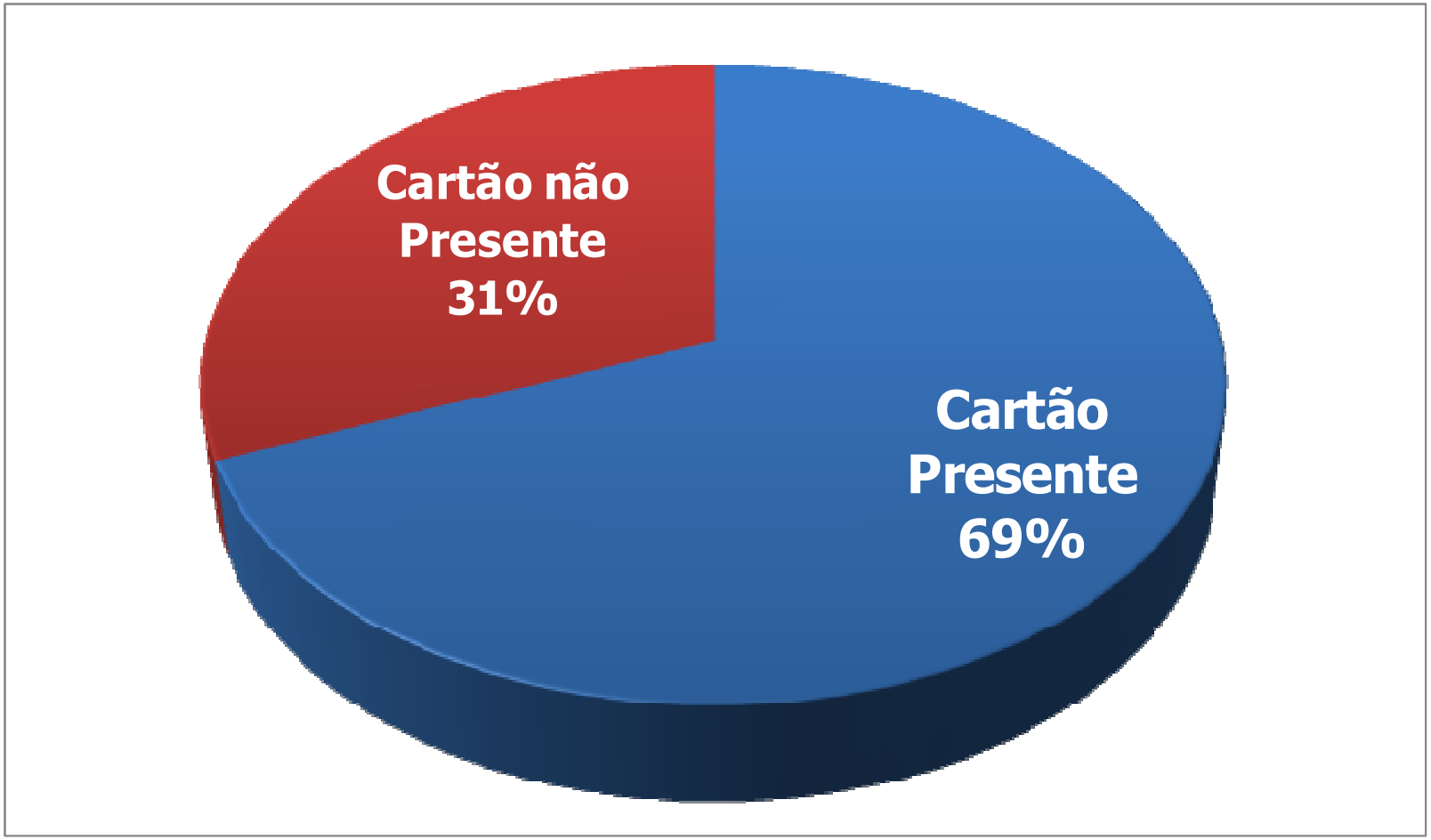
Now you can buy Visa

Estatística: Nível dos Comércio

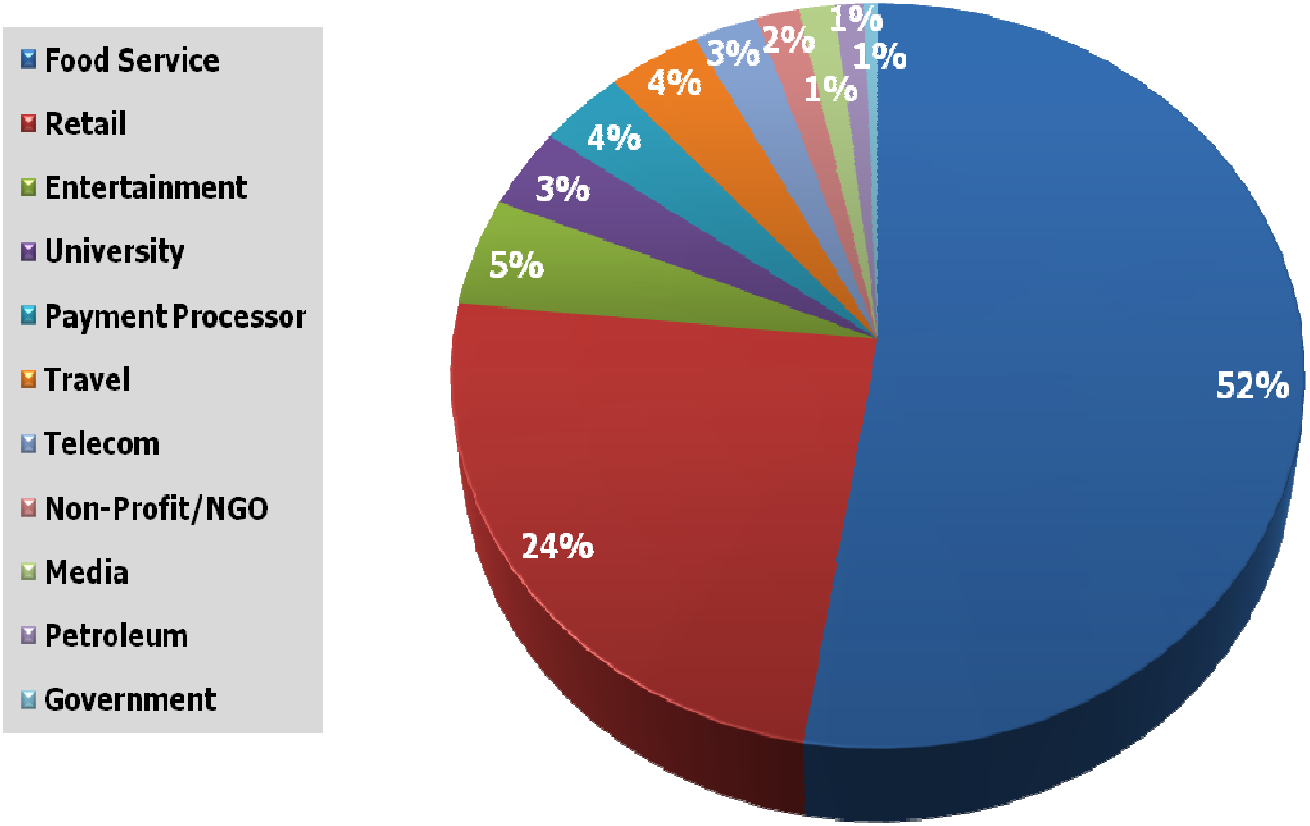


Os dados que serão apresentados são derivados de mais de 350 investigações forenses , em casos onde os dados do portador do cartão foram comprimetidos, realizadas em mais de 14 países diferentes pela Trustwave. Não há dados do Brasil.

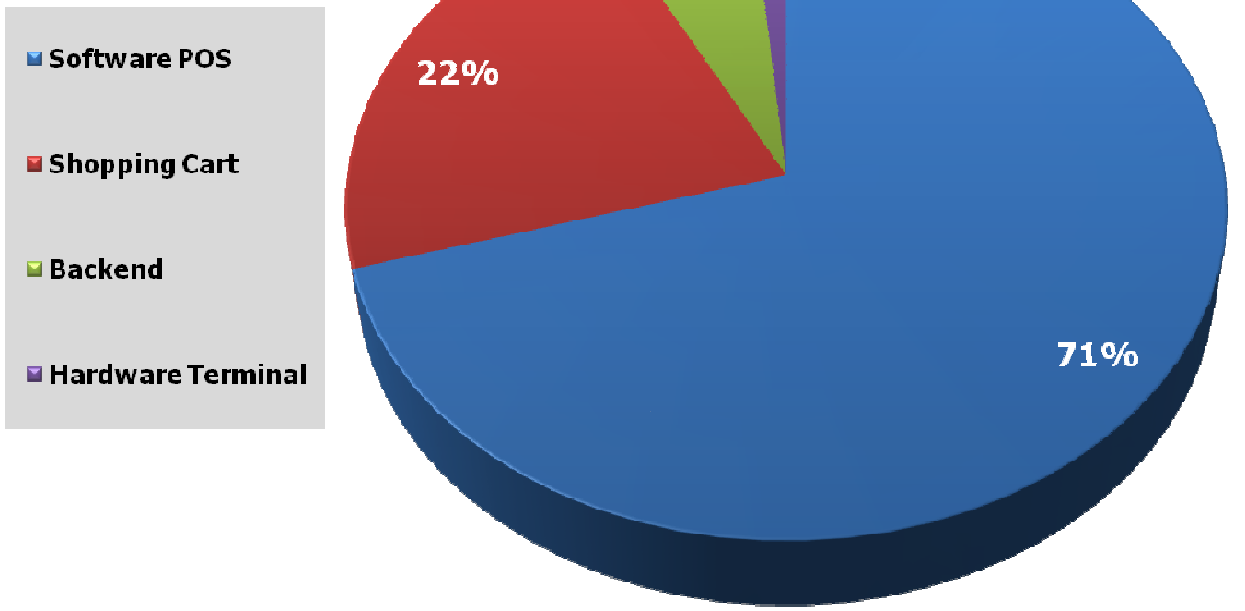
Estatística: Tipo de Aceitação



Estatística: Segmento da Indústria



Estatística: Tipo de Sistema



Software POS é um sistema que é executado em um computador de lojas. No **Brasil** é conhecido simplesmente como **PDV**.

Shopping Cart é uma ferramenta utilizada em comércios eletrônicos para facilitar os consumidores a interagirem com os produtos durante uma compra online.

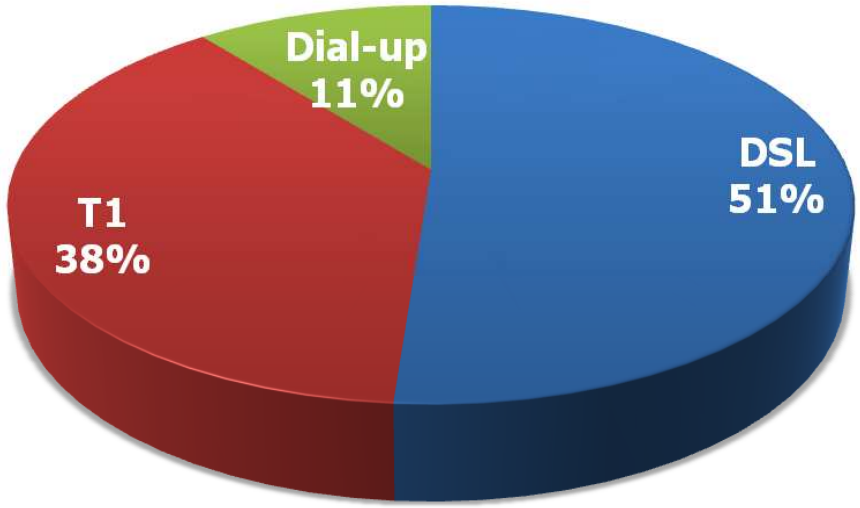
Backend é um sistema de processamento centralizado usado pelos comerciantes para agregar as transações de vários Softwares POS. No **Brasil** é conhecido como **Concentrador**.

Hardware Terminal é um dispositivo dedicado utilizado pelos comerciantes para substituir o Software POS. Muito comum em restaurantes. No **Brasil** é conhecido somente por **POS**.

Nenhuma dessas aplicações estava em conformidade com Visa PABP ou PCI PA-DSS

Estatística: Conectividade Externa

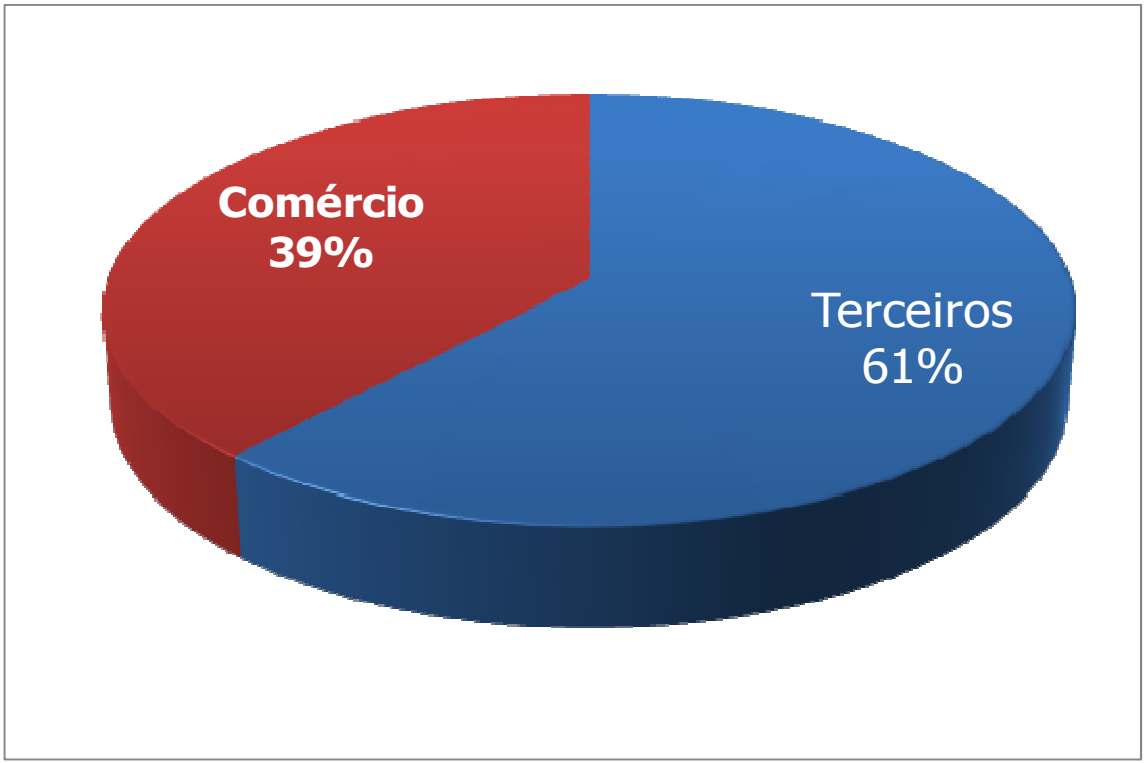
Uma alta porcentagem dos comprometimentos é devida a configuração errada de soluções de acesso remoto.



Todas as conectividades com a Internet deveriam ser consideradas de ALTO RISCO

Estatística: Responsabilidade pelos Erros

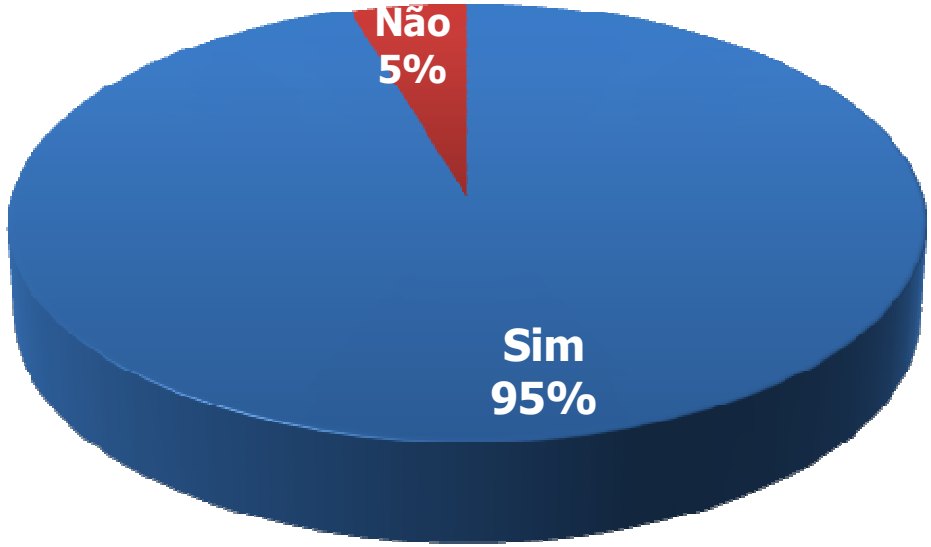
Mais da metade dos compromentimentos foi causado por falhas no serviço prestado por Terceiros aos Comércios.



Desenvolvedores de PDV, Integradores e Empresas de TI, que não estão seguindo o PCI DSS, estão deixando os comérios em Risco!

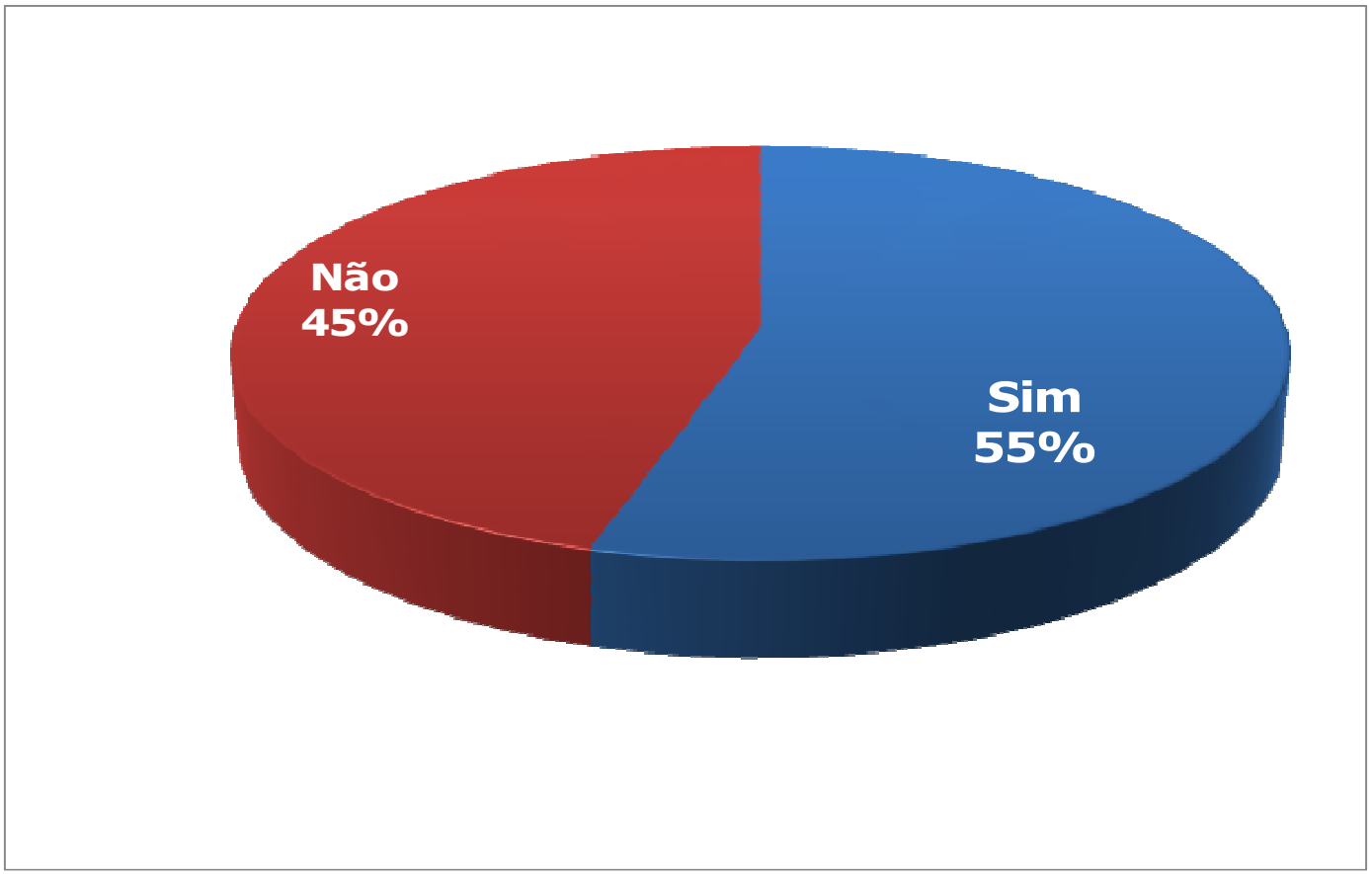
Estatística: Armazenamento da Trilha Completa

Varejistas que utilizam softwares Não-Conformes estão armazenando dados da trilha completa e quando descobrem já é muito tarde!



Armazenamento dos Dados da Trilha Completa Nunca é Permitido, em qualquer ambiente, após a autorização.

Estatística: Armazenamento do Código de Segurança



Armazenamento do Código de Segurança após a autorização nunca é permitido.

PCI SSC

- PCI SSC é uma organização fundada por American Express, Discover Financial Services, JCB International, MasterCard Worldwide e Visa Inc.
- O Conselho de Padrões de Segurança da Indústria de Cartões de Pagamento (PCISSC) é uma entidade independente que define os requerimentos técnicos e de negócio de como os dados de pagamento devem ser armazenados e protegidos (PCI DSS). O PCISSC é também responsável por estabelecer os critérios para os Qualified Security Assessors (QSAs) e Approved Scanning Vendors (ASVs).
- https://www.pcisecuritystandards.org/
- PCI DSS (Data Security Standard) 1.1

Políticas das Bandeiras vs. PCI

- Cada bandeira (Visa, Mastercard, American Express, Discover e JCB) define sua própria política de conformidade e quando o padrão PCI deve ser aplicado
  - Visa USA: CISP (Cardholder Information Security Program)
  - Outras Regiões da Visa: AIS (Account Information Security)
  - MasterCard: SDP (Site Data Protection)
  - American Express: DSOP (Data Security Operating Policy)
  - Discover: DISC (Data Information Security Compliance)
  - JCB: DSP (Data Security Program)
- Essas políticas das bandeiras cobrem:
  - Para quem os padrões técnicos do PCI se aplicam
  - Definições dos níveis de classificação
  - Requerimentos de conformidade (ex:. datas), penalidades e multas

Padrão de Segurança de Dados

	Data Element	Storage Permitted	Protection Required	PCI DSS Req. 3.4
Cardholder Data	Primary Account Number (PAN)	YES	YES	YES
	Cardholder Name*	YES	YES*	NO
	Service Code*	YES	YES*	NO
	Expiration Date*	YES	YES*	NO
Sensitive Authentication Data**	Full Magnetic Stripe	NO	N/A	N/A
	CVC2/CVV2/CID	NO	N/A	N/A
	PIN / PIN Block	NO	N/A	N/A

*** These data elements must be protected if stored in conjunction with the PAN. This protection must be consistent with PCI DSS requirements for general protection of the cardholder environment. Additionally, other legislation (for example, related to consumer personal data protection, privacy, identity theft, or data security) may require specific protection of this data, or proper disclosure of a company's practices if consumer-related personal data is being collected during the course of business. PCI DSS, however, does not apply if PANs are not stored, processed, or transmitted.**

**** Sensitive authentication data must not be stored subsequent to authorization (even if encrypted).**

Seis Metas: Doze Requerimentos – PCI DSS

Meta 1: Construa e Mantenha uma Rede Segura

Requerimento 1: Instale e mantenha uma configuração de firewall para proteger os dados do portador de cartão

Requiremento 2: Não use as senhas padrão de sistema e outros parâmetros de segurança fornecidos pelos prestadores de serviços

Meta 2: Proteja os Dados do Portador de Cartão

Requerimento 3: Proteja os dados armazenados do portador de cartão

Requerimento 4: Codifique a transmissão dos dados do portador de cartão nas redes públicas e abertas

Seis Metas: Doze Requerimentos – PCI DSS

Meta 3: Mantenha um Programa de Administração da Vulnerabilidade

Requerimento 5: Use e atualize regularmente o software ou programas antivírus

Requerimento 6: Desenvolva e mantenha sistemas e aplicativos seguros

Meta 4: Implemente Medidas Rígidas de Controle de Acesso

Requerimento 7: Restrinja o acesso aos dados do portador de cartão a apenas aqueles que necessitam conhecê-los para a execução dos trabalhos

Requerimento 8: Atribua um ID único para cada pessoa que possua acesso ao computador

Requerimento 9: Restrinja o acesso físico aos dados do portador de cartão

Seis Metas: Doze Requerimentos – PCI DSS

Meta 5: Acompanhe e Teste Regularmente as Redes

Requerimento 10: Acompanhe e monitore todo o acesso aos recursos da rede e dados do portador de cartão

Requerimento 11: Teste regularmente os sistemas e processos de segurança

Meta 6: Mantenha uma Política de Segurança da Informação

Requerimento 12: Mantenha uma política que atenda à segurança da informação para funcionários e prestadores de serviços

Principais Violações do PCI DSS

Req.1: Segmentação de Redes

Req. 3: Armazenamento de Dados

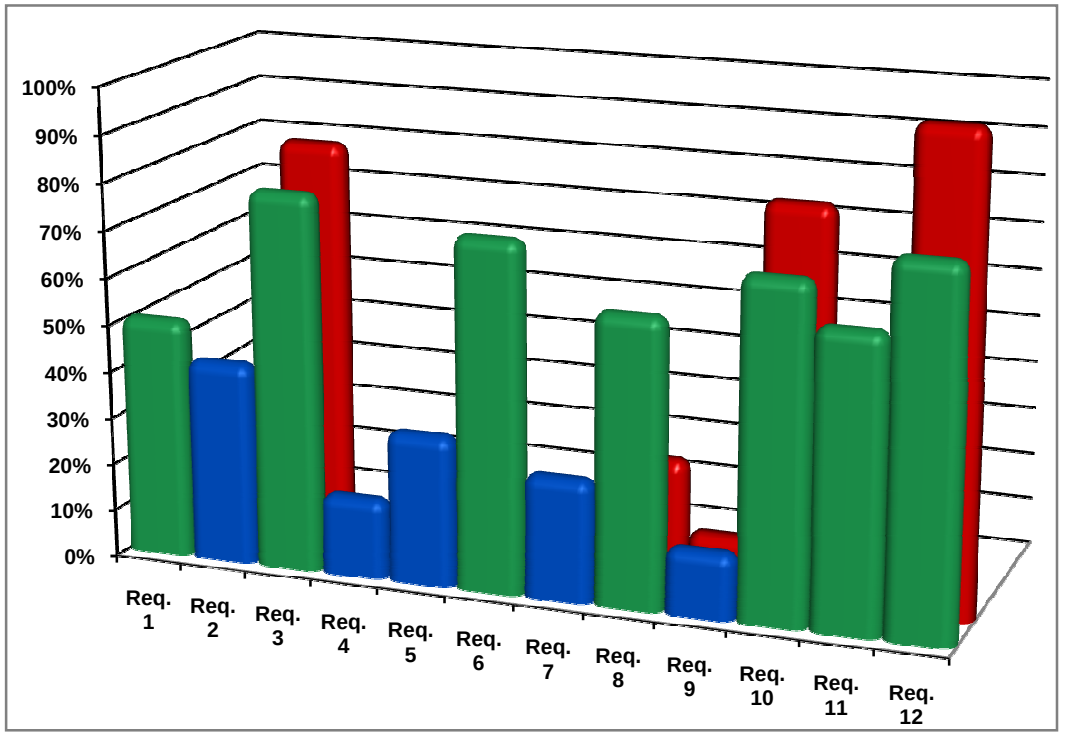
Req. 6: Desenvolvimento de Aplicações

Req. 8: Credenciais

Req. 10: Monitoração e Logs

Req. 11: Testes

Req. 12: Políticas de Segurança



Violações >50% Encontradas durante investigações forense

Violações <50% Encontradas durante investigações forense

Violações encontradas durante a fase inicial de uma auditoria PCI-DSS

Trustwave® Information Security & Compliance

Trustwave®
Information Security & Compliance

Perguntas?