Subject: Re: [sacm] [mile] Strategic alignment of security with business in SACM in an international context
Date: Thursday, August 16, 2012 12:16:24 AM Pacific Daylight Time
From: Moriarty, Kathleen (sent by <sacm-bounces@ietf.org>)
To: John Howie, Luis Nunez, Waltermire, David A.
CC: Ruben Oliva, mile@ietf.org, sacm@ietf.org, Becky Swain

Thank you very much for the disclosure and offer, this could be extremely helpful!

We will also need a form filled in on the IETF site for the disclosure, I'll email you separately.

Thank you,
Kathleen

____
From: mile-bounces@ietf.org [mile-bounces@ietf.org] On Behalf Of John Howie [jhowie@cloudsecurityalliance.org]
Sent: Wednesday, August 15, 2012 12:39 AM
To: Luis Nunez; Waltermire, David A.
Cc: Ruben Oliva; mile@ietf.org; sacm@ietf.org; Becky Swain
Subject: Re: [mile] [sacm] Strategic alignment of security with business in SACM in an international context

Hi all,

The Cloud Security Alliance intellectual property, including the Cloud Controls Matrix, can be used royalty free with attribution, should you wish to use it. We are making some updates to the Cloud Controls Matrix, and I have Cc'ed Becky Swain who can answer any questions you might have about the updates.

Regards,

John
[cid:A936CCB9-0FA0-4F17-97F6-B45ABC11EFA3]

From: Luis Nunez <lnunez@c3isecurity.com<mailto:lnunez@c3isecurity.com>>
Date: Wednesday, August 8, 2012 9:50 AM
To: "Waltermire, David A." <david.waltermire@nist.gov<mailto:david.waltermire@nist.gov>>
Cc: Ruben Oliva <david.oliva@verizon.net<mailto:david.oliva@verizon.net>>,
<mile@ietf.org<mailto:mile@ietf.org>>, <sacm@ietf.org<mailto:sacm@ietf.org>>
Subject: Re: [mile] [sacm] Strategic alignment of security with business in SACM in an international context

I had mention the Cloud Security Matrix (Cloud Security Alliance) in another thread.
1. is this something we can use as basis for mapping the various regulations to a common id?
2. Is this SACM or MILE GRC related work?

thanks.
-ln

On Aug 8, 2012, at 12:37 PM, Waltermire, David A. wrote:

The challenge we will likely face in scoping down the effort is that we might not be able to work on the full stack that supports low-level data collection, as well as higher level security processes and controls. This is because we will likely need to charter around a lower layer of function. This is why we need to scope as part of this work an architecture document that illustrates how the smaller scope of work fits into the larger picture that supports alignment with international compliance models.

To say it a different way, we need to define a comprehensive picture of the “end state”, even though we may only get part way there based on an initial SACM charter.

We can use documents like ISO 27001 as guidance in producing the architecture document to insure that the end state aligns well with your concerns below.

Sincerely,
Dave

From: sacm-bounces@ietf.org<mailto:sacm-bounces@ietf.org> [mailto:sacm-bounces@ietf.org] On Behalf Of david.oliva@verizon.net<mailto:david.oliva@verizon.net>
Sent: Wednesday, August 08, 2012 10:22 AM
To: lnunez@c3isecurity.com<mailto:lnunez@c3isecurity.com>; sacm@ietf.org<mailto:sacm@ietf.org>
Subject: [sacm] Strategic alignment of security with business in SACM in an international context

Luis and all:
Unless we can demonstrate that the technologies and specifications we are developing align with the security objectives of international compliance models (such as ISO 27001) we cannot demonstrate strategic alignment of business and security objectives in their context.
Strategic alignment of security objectives with business objectives can be at least partially joined via SACM thru the SP 800-53 to ISO 27001 mapping table. If this were to happen to SACM then the validated products will have less appeal and less marketability. The validated products will work fine, but they will work with limited capability and scope. For example, currently validated SCAP 1.0 products do not use the Open Checklist Interactive Language (OCIL). OCIL is an open specification (created by the security community for use by anybody, any developer, any country) that facilitates non-automated assessment of security processes. OCIL would allow an ISO 27001 compliance assessor in Germany to create a question “Does the organization comply ISO/IEC 27001:2005 para 4.2.2 e) ‘Does the organization implement a training and awareness programme’” and answer ‘yes’ or ‘no’. Then the results can be accessed and read whether the organization uses product X or product Y because OCIL is an open security specification. Another example of OCIL is a rather mundane security function of universal use. OCIL allows an ISO 27001 security compliance officer to answer ‘yes’ or ‘no’ to the question “Is the door shut?” and make the result electronically readable whether he/she uses product X or product Y. As for business, the flexibility of OCIL allows a company to create a question “Did the company reach our 7% profit strategic objective over the past 10 years?” and able to answer it ‘yes’ or ‘no’ with product X, Y, or Z and ensure interoperability.

David Oliva

On 08/07/12, Luis Nunez<lnunez@c3isecurity.com<mailto:lnunez@c3isecurity.com>> wrote:

Thanks the comment. I am glad someone agrees with me :)

-ln

On Aug 7, 2012, at 11:46 AM, david.oliva@verizon.net<mailto:david.oliva@verizon.net> wrote:

Luis and all:

You are on target.
SACM is not a law enforcement thing, but is a facilitator of legal issues in association with the protection of private information and health-related information.
I think a couple of examples to show how SACM facilitates legal issues about personal information is in order.

A SACM configuration scanner is able to monitor the configuration of security controls as specified in ISO/IEC 27001:2005. This can be accomplished when tier IV SCAP content is used because the output maps the finding (compliance or non-compliance) of the scanner to security control ISO/IEC 27001:2005 paragraph A.10.6.2 “Security of Network Services”. Thus a SACM scanner is able to assist in international governance compliance about personal information because SP 800-53 maps to ISO 27001.
A SACM vulnerability scanner is able to meet compliance with ISO 27001, para A.12.6.1 “Control of technical vulnerabilities” because a SACM scanner using SCAP tier IV content can map its output to the ISO governance. SACM Vulnerability scanning can address aspects of confidentiality of personal information by identifying software vulnerabilities of the databases that house them, and do it in the context of an international set of security standards.

David Oliva

On 08/06/12, Luis Nunez<lnunez@c3isecurity.com<mailto:lnunez@c3isecurity.com>> wrote:

Looking at it another way I could see security automation as a way to discover if a system is configured to meet privacy policies .

Security automation is an enabler for transparency so that individuals and organizations may understand the complex computing environment.

Thanks for bring up this issue. As a community we may want to look at building content around privacy controls.

-ln

On Aug 6, 2012, at 12:42 PM, <Kent_Landfield@McAfee.com<mailto:Kent_Landfield@McAfee.com>> wrote:

None of the efforts we are talking about for SACM are targeted toward PII or individuals. They are targeted at the configuration of the platforms deployed in the enterprise to assure they comply with the site's security policy. PII is not collected. This is not monitoring of individual or employee actions. I am not a lawyer and will not speak as one. We will let the lawyer's decide at the appropriate time.

Kent Landfield

McAfee | An Intel Company
Direct: +1.972.963.7096
Mobile: +1.817.637.8026
Web: www.mcafee.com<http://www.mcafee.com/>

From: Martin Rex <mrex@sap.com<mailto:mrex@sap.com>>
Reply-To: "mrex@sap.com<mailto:mrex@sap.com>" <mrex@sap.com<mailto:mrex@sap.com>>
Date: Monday, August 6, 2012 11:32 AM
To: "tony@yaanatech.com<mailto:tony@yaanatech.com>" <tony@yaanatech.com<mailto:tony@yaanatech.com>>
Cc: "mrex@sap.com<mailto:mrex@sap.com>" <mrex@sap.com<mailto:mrex@sap.com>>, "sacm@ietf.org<mailto:sacm@ietf.org>" <sacm@ietf.org<mailto:sacm@ietf.org>>
Subject: Re: [sacm] Legal aspects of System monitoring

Tony Rutkowski wrote:
Martin Rex wrote:

In Germany, an employer monitoring a company-owned PC that an employee uses for communication (EMail, VoiP, IM) would be unconditionally illegal.

Really?

No kidding!

That is not consistent with comments
I've seen concerning German law.

There is a significant amount of mis-information floating the internet.
And a mindboggling large number of lawyers are making wild guesses, rather
that doing research.

The decisions of the german federal constitional court (GFCC) have been
quite consistent over the past decade about what with respect to
encroaching on the general right of personality, informational
self-determination, freedom of conduct and created a "fundamental right
to the guarantee of the integrity and confidentiality of information
technology systems". The court has set the minimum requirements that
are prerequisite to such encroachment, such as the prerequisite of a
clear formal statute law, which needs to be limited to situation where
real facts create probable cause.

The original GFCC decision in german language is quite comprehensible
(to me, at least), while I'm having some difficulties understanding
the english translation (and the english translation is shorter!?).

BVerfG-Entscheidung "1 BvR 370/07 vom 27.2.2008" Randnummer 196-
http://www.bverfg.de/entscheidungen/rs20080227_1bvr037007.html#abs196

english translation of "1 BvR 370/07 vom 27.2.2008"
http://www.bverfg.de/entscheidungen/rs20080227_1bvr037007en.html#abs130

To be *unconditionally* illegal, would
preclude almost any rationally required
maintenance or threat mitigation.

It is possible to perform maintenance and threat mitigation entirely
without "monitoring" systems.

A mere threat is insufficient for monitoring, if that involves collecting
PII data, i.e. data from which a persons conduct can be infered.

It is fair to observe that recent German
Constitutional Court decisions impose
constraints, but they certainly are
not "unconditional."

One of the prerequisite is a clear formal statute law, which currently does not exist for the purposes "sacm" is about.

quoting from the above GFCC decision:

> 2. The fundamental right to the guarantee of the confidentiality and integrity of information technology systems is not unrestricted. Encroachments may be justified both for preventive purposes, and for criminal prosecution. The individual must only accept such restrictions of his or her right which are based on a statutory foundation that is constitutional.

This currently makes collecting data about peoples conduct "unconditionally" illegal for most practical purposes (exempting from prosecution only individual occasions of justified self-defence against an imminent vicious attack based on real facts that create probable cause).

This applies to all surveillance that impairs persons "freedom of conduct". The majority of past decisions of specific events was about surveillance with a camera, but the GFCC decision makes it crystal clear that this applies to *any* kind of surveillance. Different to monitoring of computer systems, there is statutory law for camera surveillance, that allows optical surveillance under certain conditions (Art. 6b BDSG "BundesDatenSchutzGesetz).

The lack of a formal statutory foundation makes surveillance illegal and entitles subjects to "cease and desist" rulings and sometimes damages.

In one more recent (and constitutionally correct) rulings, an employer had put up a camera that had in view not only the entrance door, but also two workplaces. The employees protested against this camera, but the employer would not "fix" it, so at least one employee sued, The court confirmed that this camera surveillance at the workplace was illegal due to its chilling effect alone, and since it had been installed for a whole year, the employee was arwarded 4 month of income as damages (for the chilling effect).

Another recent decision was about evidence from a covert video surveillance showing an employee taking a package of cigarettes on two occasions, where the German Federal Labour Court (the supreme court for labor related issues) remanded the decision to the trial court because it had failed to establish whether the covert video surveillance really met all constitutional prerequisites otherwise the video surveillance would have been illegal and not be admissible as evidence in court.
(German decision: http://lexetius.com/2012,2351)

The German Federal Constitional Court neutered numerous laws during the last decade due to lack of clarity and/or overbroad encroachment of the personal right of self-determination and the right to confidentiality of telecommunications.

See also the GFCC decision about the scanning of license plates

(the decision 1 BvR 2074/05 vom 11.3.2008 in german)
http://www.bverfg.de/entscheidungen/rs20080311_1bvr2-07405.html

where it confirmed that data collection requires formal statue law,
and that the law in question wasn't limited to probable cause and
therefore unconstitutional.

The only currently existing formal statue law in Germany, that could be used in some limited fashion for "Monitoring" is Art.100 TKG,
http://www.gesetze-im-internet.de/tkg_2004/__100.html
but that statue is clearly limited in purpose, it will not allow that data to be used for automatic surveillance of "employee conduct" with respect to "company-defined policies". Employers try hard to avoid TKG for their networks (for which they will have to formally register), but that also means that they do not have a formal statutory law for performing any kind of surveillance/monitoring as described in Art. 100 TKG for systems that are used by employees for telecommunications and a significant part of their daily activies.

-Martin
____
sacm mailing list
sacm@ietf.org<mailto:sacm@ietf.org>
https://www.ietf.org/mailman/listinfo/sacm

____
sacm mailing list
sacm@ietf.org<mailto:sacm@ietf.org>
https://www.ietf.org/mailman/listinfo/sacm

____

____
sacm mailing list
sacm@ietf.org<mailto:sacm@ietf.org>
https://www.ietf.org/mailman/listinfo/sacm

____ mile mailing list mile@ietf.org<mailto:mile@ietf.org>
https://www.ietf.org/mailman/listinfo/mile

____
sacm mailing list
sacm@ietf.org
https://www.ietf.org/mailman/listinfo/sacm