Message

From: Fryer, Teresa M. (CMS/OIS) NotResp
NotResp

Sent: 11/1/2013 12:09:33 AM

To: Trenkle, Tony (CMS/OIS) NotResp
NotResp
NotResp
Schankweiler, Thomas W. (CMS/OIS) NotResp

CC: Linares, George E. (CMS/OIS) NotResp
NotResp Outerbridge, Monique (CMS/OIS) NotResp
NotResp rothe, Kirk A. (CMS/OIS) NotResp
NotResp King,
Terris (CMS/O NotResp Robinson, Carolyn
E. (CMS/OIS NotResp Marantan,
James (CMS/OIS) NotResp

Subject: RE: PenTesting tonight - I need help... please.

Sensitivity: Company Confidential

Yes I agree that there are conflict of interest issues since NotResp is involved with the development of the NotResp nd we have been conducting authenticated scans of the internet facing web servers (which is an extensive list) of the Marketplace systems (not just healthcare.gov). There also needs to be rules of engagement in place and signed by appropriate parties.

From: Trenkle, Tony (CMS/OIS)
Sent: Thursday, October 31, 2013 6:40 PM
To: Schankweiler, Thomas W. (CMS/OIS)
Cc: Linares, George E. (CMS/OIS); Outerbridge, Monique (CMS/OIS); Grothe, Kirk A. (CMS/OIS); Fryer, Teresa M. (CMS/OIS); King, Terris (CMS/OIS); Robinson, Carolyn E. (CMS/OIS)
Subject: Re: PenTesting tonight - I need help... please.

Tom

NotResp

Teresa

Do you know anything about this?

From: Schankweiler, Thomas W. (CMS/OIS)
Sent: Thursday, October 31, 2013 06:34 PM
To: Trenkle, Tony (CMS/OIS)
Cc: Linares, George E. (CMS/OIS); Outerbridge, Monique (CMS/OIS); Grothe, Kirk A. (CMS/OIS); Fryer, Teresa M. (CMS/OIS)
Subject: PenTesting tonight - I need help... please.

Tony, e.t. all,

NotResp is running a pen-test tonight against healthcare.gov (english). Presumably this was a request that came from Marilyn Tavener. The test is non-authenticated and is supposed to look for basic NotRes vulnerabilities.

Tomorrow there is supposed to be a larger discussion (no meeting scheduled yet) about releasing all the security documentation and vulnerability information to [NotResp] in support of a project they are doing. I just wanted to confirm with [NotResp] leadership that everyone is aware of this request and that it ok to release all of this sensitive information. I am hyper-sensitive about this situation and really don't want to release all of this data especially to the same group that is doing Hub security for [NotResp] (where is the whole separation of duties here?).

I am also concerned that we are getting hit with multiple requests to do the same thing repeatedly without a grand strategy. here is what I mean...

- HHS CSIRC has been on-site and reviewed and verified the program and open findings
- HHS CSIRC wants to scan weekly, and now has access to [NotResp] and will soon have access to the [NotResp] and the [NotResp] and the [NotResp]
- [NotRe] has been tasked to independently investigate the independent findings from HHS which they got from the [NotResp] which is also independent of the developers. (that's three levels of independence)
- [NotResp] is conducting weekly scans
- We are preparing for the next [NotResp] test which is an end-to-end strategy
- [NotResp] is testing daily and working with developers
- We are getting hit by hackers, journalists, and other tester companies throwing darts at us
- Now there is testing by [NotResp]

This is just a lot to keep up with and respond to. Also our confidential and sensitive information is growing legs and going way beyond the normal borders, which has actually led to some of the recent security incidents. I need some executive cover here, and backing to ensure we are working with a strategy and have boundaries for releasing information.

Thanks,

Tom

Message

From:	Fryer, Teresa M. (CMS/OIS)	NotResp

NotResp

Sent:	11/1/2013 12:03:38 AM

To:	Trenkle, Tony (CMS/OIS	NotResp

NotResp | Schankweiler, Thomas W. (CMS/OIS) | NotResp

NotResp

CC:	Linares, George E. (CMS/OIS)	NotResp

NotResp | Outerbridge, Monique (CMS/OIS) | NotResp

NotResp | Grothe, Kirk A. (CMS/OIS) | NotResp

NotResp | King,

Terris (CMS/OIS | NotResp | Robinson, Carolyn

E. (CMS/OIS | NotResp

Subject:	RE: PenTesting tonight - I need help... please.

Sensitivity:	Company Confidential

No I have not heard anything about this.

From: Trenkle, Tony (CMS/OIS)
Sent: Thursday, October 31, 2013 6:40 PM
To: Schankweiler, Thomas W. (CMS/OIS)
Cc: Linares, George E. (CMS/OIS); Outerbridge, Monique (CMS/OIS); Grothe, Kirk A. (CMS/OIS); Fryer, Teresa M. (CMS/OIS); King, Terris (CMS/OIS); Robinson, Carolyn E. (CMS/OIS)
Subject: Re: PenTesting tonight - I need help... please.

Tom

This is first I have heard of this and don't think that Marilyn would be ordering a security test. Is that what they told you? Who told you this and who is setting up the meeting?

Teresa

Do you know anything about this?

From: Schankweiler, Thomas W. (CMS/OIS)
Sent: Thursday, October 31, 2013 06:34 PM
To: Trenkle, Tony (CMS/OIS)
Cc: Linares, George E. (CMS/OIS); Outerbridge, Monique (CMS/OIS); Grothe, Kirk A. (CMS/OIS); Fryer, Teresa M. (CMS/OIS)
Subject: PenTesting tonight - I need help... please.

Tony, e.t. all,

NotResp is running a pen-test tonight against healthcare.gov (english). Presumably this was a request that came from Marilyn Tavener. The test is non-authenticated and is supposed to look for basic NotResp vulnerabilities.

Tomorrow there is supposed to be a larger discussion (no meeting scheduled yet) about releasing all the security documentation and vulnerability information to NotResp in support of a project they are doing. I just wanted to confirm with NotResp leadership that everyone is aware of this request and that it ok to release all of this sensitive information. I am hyper-sensitive about this situation and really don't want to release all of this data especially to the same group that is doing Hub security for NotResp (where is the whole separation of duties here?).

I am also concerned that we are getting hit with multiple requests to do the same thing repeatedly without a grand strategy. here is what I mean...

- HHS CSIRC has been on-site and reviewed and verified the program and open findings
- HHS CSIRC wants to scan weekly, and now has access to [NotResp] and will soon have access to the [NotRes] and the [NotResp], and the [NotResp]
- [NotResp] has been tasked to independently investigate the independent findings from HHS which they got from the [NotResp] which is also independent of the developers. (that's three levels of independence)
- [NotRe]s conducting weekly scans
- We are preparing for the next [NotResp] test which is an end-to-end strategy
- [NotResp] is testing daily and working with developers
- We are getting hit by hackers, journalists, and other tester companies throwing darts at us
- Now there is testing by [NotResp]

This is just a lot to keep up with and respond to. Also our confidential and sensitive information is growing legs and going way beyond the normal borders, which has actually led to some of the recent security incidents. I need some executive cover here, and backing to ensure we are working with a strategy and have boundaries for releasing information.

Thanks,

Tom