Security Professionals Conference 2X18

Security and Privacy Professionals: All Hands on Deck!

All for One and One for All

Wednesday, April 11, 2018, 4pm ET
All for One and One for All: EDUCAUSE, Internet2, and REN-ISAC's Swashbuckling Adventures in Cybersecurity
Today’s Musketeers

- Joanna Grama, EDUCAUSE
- Todd Herring, REN-ISAC
- Paul Howell, Internet2
- Nick Lewis, Internet2
- Kim Milford, REN-ISAC
- Valerie Vogel, EDUCAUSE
Agenda

• Who are we and why are we here?
• Collaborative Successes!
• Who is steering the ship?
• What’s going on?
• Your feedback!
Changes to our guidelines to allow membership to:

- Executives with a stake in InfoSec
- Security practitioners in roles such as IAM, risk management, ERP systems
## REN-ISAC: CSIRT Activities

<table>
<thead>
<tr>
<th>First Quarter Notifications</th>
<th>2018</th>
<th>2017</th>
</tr>
</thead>
<tbody>
<tr>
<td>Compromised Machines</td>
<td>16,083</td>
<td>14,376</td>
</tr>
<tr>
<td>Compromised Credentials</td>
<td>5,008</td>
<td>1,483</td>
</tr>
<tr>
<td>Spam or Phish</td>
<td>78</td>
<td>118</td>
</tr>
<tr>
<td>Vulnerable Machines</td>
<td>0</td>
<td>27</td>
</tr>
<tr>
<td>Open Recursive DNS Resolvers</td>
<td>612</td>
<td>707</td>
</tr>
<tr>
<td>Open Mail Relays</td>
<td>14</td>
<td>39</td>
</tr>
<tr>
<td>Unique Institutions Contacted</td>
<td>1622</td>
<td>622</td>
</tr>
</tbody>
</table>
REN-ISAC CSIRT Activities

Compromised Machines: Exploits

- Ramnit
- Avalanche - Nymaim
- Zeus
- Sinkhole
- Gozi
- Mirai
- Xcode Ghost
- Avalanche - Andromeda
- Conficker
- WannaCry

#Security18
REN-ISAC: Upcoming Workshops and Exercises

• Partnering with Gate15 to conduct 6 workshops around the country
• Focus on physical security
• With a significant cyber threat
• Written reports to be shared

#Security18
Internet2

- Network security working group
  - DDoS mitigation techniques
  - Inter-domain routing security
- Coordination with Global NREN security working teams
Internet2

- DDoS Scrubbing Using Zenedge
Internet2

• **Cloud Services Updates**
  - Duo, Splunk, GCP, others
  - Incorporating HECVAT into the program

• **InCommon**
  - Baseline Expectations and SIRTFI - getting infosec and IAM working together
  - Incident Response - [2016-11-17-01](#) (InCommon IdPs release duplicate persistent nameID to ORCID SP)

• **TIER**

#Security18
The Cybersecurity Program, led by HEISC, provides resources and events to help you develop and sustain top-notch information security governance, compliance, data protection, and privacy programs.

www.educause.edu/security
Working Group Resources

Budget Conscious Information Security Resources

According to the EDUCAUSE Core Data Service, information security spending is roughly 3% of an institution's overall IT budget spending, and there are only 2 central IT information security FTEs per 10,000 institutional FTEs. Only 34% of institutions have a dedicated person whose primary job responsibility is information security. In such an environment, how can institutions that are just starting out with an information security program, or those with even more limited resources, successfully protect institutional IT resources and data?

These resources, prepared by members of the Higher Education Information Security Council, provide budget-conscious advice for IT leaders and managers tasked with developing and delivering institutional information security programs and services.

The reports below will be published in April 2018.

Collaboration Ho!

• Working Groups
  • HECVAT & CBI
• Program Committees
• Feedback on each others’ projects
• REN-ISAC Enterprise Participation
Higher Education Cloud Vendor Assessment Tool (HECVAT): Streamlining Security Risk Review

Five steps to protecting security and privacy in the cloud

**Bench**mark 1
Institution A uses HECVAT responses to ensure its service provider partners are protecting institutional systems and data appropriately.

**Bench**mark 2
Institution A wants to move to the cloud for a new LMS and identifies Wegovide 123.com to fulfill that need.

**Bench**mark 3
Institution A checks the Internet2 Cloud Services Listings and the REN-ISAC Cloud Broker Index to see if Wegovide 123.com has completed a HECVAT questionnaire for its LMS product. It has not.

**Bench**mark 4
During the procurement process, Institution A encourages Wegovide 123.com to complete a HECVAT for its LMS product, and to list that HECVAT in the REN-ISAC Cloud Broker Index.

**Bench**mark 5
Institution B is looking for a new LMS, sees that Wegovide 123.com has a HECVAT listed on the REN-ISAC Cloud Broker Index and contacts Wegovide 123.com about its product.

**HECVAT Benefits**
For Institutions:
- Consistent Security Review Process
- Cost and Resource Savings

For Service Providers:
- Cost and Resource Savings
- Lead Generation

www.educause.edu/hecvat
Who is Steering the Ship?

- *Members steer the ship!*
- We come together monthly to share our activities and make sure we are not missing collaboration opportunities.
Tell Us About It!

• What do you need? What is not getting done?
• Where do you see our coordination opportunities?
Thank you!

Please be sure to complete the evaluation for today’s event.

Your feedback helps improve both the conference and the presentations.