Cadre
information security

BUILDING THE PROPER CSIRT

How do we respond to security incidents?

Tom Ellis
Senior Security Engineer
Cadre Information Security

INTRODUCTION

- Tom Ellis, Senior Security Engineer
- 6 years with Cadre Information Security
- 25+ years of IT experience
- Systems Engineering
- Operations Management
- Project Management
- Security Engineering

SECURITY EVENTS HAPPEN

- As of 2015 80% of U.S. companies were successfully hacked in one way or another.
- The average firm loses over $15 million per year to security events.
- When it happens, building the right team and process to deal with the aftermath is crucial.
- It is better to have the plan and people in place and ready to go. Minimizing downtime or the level of compromise is crucial to business.

PLANNING A RESPONSE

- Response time is critical. Having the right team in place is crucial to managing security incidents.
- Management support is crucial. A sponsor is an important component to a response team.
- Proper planning is a must have piece of any response plan. Just having a team in place isn't always enough.
- Discovery and information gathering is a critical piece of a response plan.
- A sound strategic plan will help alleviate pain. Ask the right questions first.

PLANNING A RESPONSE

- What are the timeframes involved where downtime has a cost?
- Gather relevant information. Meet with stakeholders. Understand the business drivers that are impacted by network security events.
- How do you communicate events to the rest of your organization?
- Collecting data during the response can be key to dealing with future incidents.

PLANNING A RESPONSE

- Legal implications can be real. The legal department should be part of any discussions on how to respond to security events.
- All aspects of Information Technology groups should be taken into account. What ramifications are there to infrastructure when an event occurs?
- How will risk be managed? Does there need to be PR, Audit, or Risk Management department involvement?
- If there is financial risk, how is that communicated and managed?

DESIGN YOUR VISION

- A clear agreement between stakeholders and the security team needs to be reached.
- Any CERT/CSIRT needs to have a clear mission plan.
- Periodic meetings to discuss the threat landscape and adjust existing plans are a must.
- How will the team be organized?
- How will the team be funded?
- Once designed it is important to communicate CSIRT process to stakeholders as it is being developed.

IMPLEMENTATION

- Identify the staff who will respond to events. Do you need to hire specific skill sets?
- Provisioning the team properly is key. Do you need software, hardware, or services to implement this properly?
- Policies and procedures. These are also key factors.
- Incident tracking.

COMMUNICATION

- How are events reported?
- Who gets reports, and what level of disclosure do those individuals get?
- Once a team is formed it should be clearly communicated to stakeholders who the people are and their purpose.
- Routine reports to stakeholders help show the value of the team.

ONGOING WORK

- It is not a static process.
- Periodic reviews of the team, events, and process will help ensure effective delivery.
- Understand the business and the inherent risks. Tailoring a response team will make it more effective and reduce overall costs.

CONCLUSION

- Any Questions?
- I can be reached at tom.ellis@cadre.net
- Contact your Cadre sales representative
  - Chris Loughner, Enterprise Security Consultant, chris.loughner@cadre.net
  - David Scott, SMB Security Consultant, david.scott@cadre.net