GFCE
Global Forum on Cyber Expertise

Global Good Practices

Practice: Assist with cyber-risk mitigation and keep score of successes

#Scorekeeping

Weight loss does not happen by learning theory, but by practical exercises — and certainly by keeping records of successful steps. Similarly, network operators need help with monitoring the systemic risks, providing training materials and practical experience for mitigation, but also keeping track of successful actions.

Related thematic areas:

Incident management and infrastructure protection

Culture and skills

Cooperation and community building

Of particular interest to:

Description

To prevent cyber-incidents, root cause systemic risks should be addressed rather than symptoms. However, understanding, identifying, and mitigating the systemic risks are not easy. Complete, reliable, and well-presented metrics that identify risks in particular networks need to be coupled with assistance for mitigation and continuous monitoring of the health of the network to evaluate success.

Training materials built on mitigation practices in the context of particular risks addressed can teach ISPs, as well as other organisations and policymakers, what is needed to mitigate particular vulnerabilities. **Capacity building support** developed around these materials, mitigation practices, and risks can increase the efficiency of mitigation.

Scorekeeping success through continuous measurement of the health of the network identifies improvements and mitigation efforts by various parties. It also identifies new risks, and incentivises partners to act collaboratively rather than competitively. Scorekeeping can also extend the collection of good practice for mitigation.

Actors (or who this is for)

Network operators, ISPs, and vendors bear the major responsibility for improving the health of networks. They are, therefore, the main beneficiaries of any capacity building programme and scorekeeping, which should incentivise and enable them to mitigate risks.

RIRs and CERTs communities which already provide capacity building and support to operators and policymakers, as well as capacity building institutions providing support in cybersecurity, can integrate training materials into their work.

Policymakers are also a particularly important stakeholder group, since their greater awareness about risks in the networks within their geographical area, mitigation efforts, and responsibilities of key players, may lead to better policies — both incentives and regulations — to ensure a healthier network.

The big picture

While CERTs warn about risks and assist partners with mitigation, it is the partners that must act in response to alerts. Few network operators and vendors can manage to address root causes, as there are always immediate threats facing these organisations that divert attention from analysing root causes.

Most ISPs and vendors could better apply knowledge to identify common root causes if assisted to track, identify, and understand risks in each network and at each moment, provided with training materials and capacity building for mitigation, and if score is kept about successful mitigation to commend proactive actors and share additional good practices.

Policymakers should, however, also benefit from capacity building. While they might not need to understand the details about mitigation practices, the metrics (*#HealthMetrics*), scorekeeping, and understanding the risks and responsibilities of major players, can assist them to develop a suitable policy environment to incentivise — or demand — operators and vendors to implement mitigation practices.

Instructions

Training materials are developed based on good mitigation practices, coupled with metrics pointing to specific risks for particular networks. Good practices can also be identified thanks to scorekeeping: Since the impact of mitigation efforts show up clearly in the metrics, it is possible to find which Internet service providers did the mitigation work and to record and share their practices.

Scorekeeping represents measuring the health of the network at different points in time. It is conducted by charting the improvements in metrics using timelines. Mitigation efficacy analysis is performed based on the timeline trend analysis, along with identifying the high-impact root-cause mitigation practices, and then sharing the practices with partners through training and capacity building to make them easy to replicate.

Capacity building activities should ensure the implementation of good mitigation practices. It is suggested to integrate mitigation training materials into various existing capacity building programmes through partnerships with capacity building institutions, so that a diversity of stakeholders can be targeted.

For mitigation to actually happen (e.g. re-configuring servers or replacing outdated devices), additional market incentives and regulation might be needed. These efforts can impact the governance model, as well as the market cycle; for instance, supporting vendors in examining cyber-hygiene and empowering users to demand security can in turn improve the vendor's return in the long term.

Timing

Developing a collaboration channel with capacity building institutions may take about two months. Developing trust building with data sources may take another one to two months. Preparing the training and workshop materials and delivery on mitigation techniques may take another one to two months. The materials and delivery should continuously be updated based on the data gathered for scorekeeping.

Example

The GFCE initiative CyberGreen makes the cyber-ecosystem healthier through measuring, visualising, and mitigating negative impacts. The initiative has built a library of training material, and offers assistance with training to various partners.

CyberGreen works with RIRs (APNIC, LACNIC, RIPE, etc.) and Regional CERTs (APCERT, TF-CSIRT, Africa-CERT, ITU-ARCC) in mitigation training and capacity building. The ITU uses CyberGreen metrics and training materials to encourage its members to act. Other partners (e.g. APCERT, ITU-ARCC, Africa-CERT) reference CyberGreen training materials to use for their own training. Countries in the ASEAN region, with the support of Singapore and CyberGreen, have established a regional platform to follow the health statistics of each country in the region, and to provide capacity building materials.

CyberGreen's current sponsors include JPCERT/CC, the Singapore CSA, and the UK FCO. These and other policymakers benefit from having increased visibility of the risk levels present in their countries.

Source, support, and mentoring

CyberGreen training materials: http://www.cybergreen.net/mitigation/#capacity-building-materials
Various related presentations: https://www.cybergreen.net/blog/?category=presentation

Contact CyberGreen:
https://www.cybergreen.net/contact/

Contact point:
Yurie Ito (yito@cybergreen.net)