General Guidelines

Available to businesses and government alike, describe a framework for responsibly handling security incidents, a segment of which addresses outside entities. What outside entities should be considered? Describe some considerations when communicating security breaches to them.

Amy Lawson-Gunkel

01 October 2019

Details

Every organization is going to have an incident response plan that is unique and appropriately reflects the needs of their company. The plan should contain the company's mission, their means of accomplishing the mission, and the goals they hope to obtain. The structure of the incident response program should be clearly outlined within the planning elements. The plan should be applied upon the review and approval by someone in the management team; after the initial approval, the plan should be reviewed and updated annually, at the very minimum.

Should an incident occur, the company will need to engage in some external correspondence. In order to maintain transparency, organizations will often report any breaches or attacks to the media; the most important thing to consider when working with the media, is to not reveal sensitive information. In addition to the press, the organization may/will have to work with some form of law enforcement. It is important for the incident response team to already have established a relationship with the representatives from their law enforcement teams; this will allow them to maximize their level of preparedness, should an event occur. Once an incident is under control, the organization should report the incident to an incident reporting organization. The incident reporting organization can be internal to the company; if one is not available internally, then an incident can be reported to other organizations. Now the Federal Information Security Management Act requires any Federal agency, who experiences an incident, to report their incident to the United States Computer Emergency Readiness Team (US-CERT).

The three outside entities, described above, are going to be the most important ones for an organization to reach out to; should the organization want to discuss their incident further they can reach out to the following: their internet service provider, their software vendors, or any external parties affected by the incident.

References

Chichonski, P., Millar, T., Grance, T., & Scarfone, K. (2012, August). Computer Security Incident Handling Guide. Retrieved October 1, 2019, from https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf.