Prevention: Human Defenses

Humans will always be the weakest link, so it's important to do everything to ensure that they are security conscious, but that it doesn't impact their ability to work to a point where it negatively impacts the business. Below we cover a number of different controls and exercises that are aimed at employees.

SECURITY AWARENESS TRAINING

Security awareness training should be provided to employees when they join the organization through an onboarding program and should be mandatory. This training should include aspects such as phishing emails and how to spot them, explain any applicable policies (more on this below), and what they should and shouldn't post on social media in regard to their work (please don't ever post pictures of your work badge... you're making it too easy for red teamers!). This training should be completed yearly, which will give the organization a chance to refresh everyone's knowledge, and the role they play in ensuring the organization's security is maintained. Various compliance frameworks often state the timeframes for security awareness training to be conducted to ensure full compliance.

SECURITY POLICIES

Security policies are used to protect the business from humans. These typically state what users can and cannot do when using company equipment, such as laptops or desktops, network connectivity, and even what employees can post on social media relating to their work. Most of this information will be contained with an "Acceptable Use Policy". It is common for all employees to sign an AUP when they are brought into the organization.

Examples of rules within an AUP could be:

- Employees may not visit the following websites during office hours and whilst using company equipment; pornographic sites or sites containing adult material, gambling sites, sites that sell prohibited items such as drugs or weapons.
- Employees are not permitted to download applications from the internet to the company devices (mobiles, desktops/laptops, tablets).
- Employees should not take documents, laptops or other company devices home unless they have permission from their inline manager or superior.
- Employees should not allow anyone else to use their username and password on any IT systems owned by the organization.

AUPs should also include the consequences of breaching the policy so that employees clearly understand that if they take prohibited actions, there will be some form of punishment.

Security teams will commonly refer to specific sections of the AUP when dealing with users that have breached it. An example of this would be having an email template that is sent to employees who are identified to be visiting sites that are prohibited in the AUP. This message will contain information about their activity (to show them that what they do on corporate systems or networks is monitored), and reference the section of the AUP that states employees are not allowed to conduct this activity.

Here's an example AUP policy, provided by GetSafeOnline.org.

INCENTIVES

Some organizations have started their own internal program for "security champions" – normal employees that are efficient at spotting not only phishing emails, but other aspects of the business that could cause a security concern, such as unpatched systems, suspicious activity from colleagues, or documents laying around. The rewards don't need to be money or holidays away to Hawaii, sometimes just giving them recognition and a thank you is enough to provide positive reinforcement, ensuring that they continue to be security conscious in the future. Gift cards or vouchers are another alternative that can be very cost-effective for the business.

PHISHING SIMULATIONS

Phishing simulations should be conducted quarterly (every 3/4 months) to test how effective the current security awareness program is. By sending phishing emails to employees that are harmless (URLs will simply take recipients to a page that states "you have been phished!") it is clear for the security team to see which users repeatedly fall for phishing emails, and need to receive additional training. This activity can generate extremely valuable metrics, such as the number of emails reported, the number of employees that have clicked the (non) malicious link, and repeat offenders. Different styled emails can be sent to different departments in more specialized cases, and targeting the C-suite should be done every now and again to ensure that everyone in the business, regardless of their position, is able to spot and report suspicious emails.

Some great platforms for doing this include:

- Sophos Phish Threat – Link
- GoPhish Open-Source – Link
- Trend Micro's Phish Insight – Link
- PhishingBox – Link

WHISTLEBLOWING

Every organization should provide an anonymous way for employees to tip off the security team about another employee if they are behaving suspiciously or maliciously. Having it anonymous means that employees know that the suspect won't know it's them, making them more likely to speak up about anything they've noticed. This can really help to ensure the security team is aware of any insider threats before they materialize and cause damage.

Previous Topic
Mark Complete
Back to Lesson