APPGUARD

The Human Side of Breach Avoidance & Readiness: 10 PRO TIPS

While most cybersecurity weaknesses involve technology, cybersecurity is ultimately a people problem. The human element exposes an enterprise to risks, undermines the effectiveness of technology, yet it can also mitigate what technology cannot. Some cyber problems are best dealt with a human solutions or at least consideration for the human condition.

We are providing ten pro tips for mitigating security gaps. This will help alleviate workloads and pressure from many layers of your cyber program.

1

Hunt for Exposed Miscellaneous Errors

As per Verizon DBIR 2019, “Miscellaneous Errors” were among the Top 3 patterns for breaches in Financial & Insurance, Education, Healthcare, Information, Public Administration, Retail, and Professional Technical/Scientific Services.

PRO-TIP

Only redundant, proactive processes can treat these human-caused symptoms. Employees should be maintaining and seeking top 10/25/100 lists on what ‘errors’ they should hunt. Collaborate with peers to maintain these lists. Prioritize thigh-impacts vulnerabilities. Seek ways to compartmentalize to reduce exposures.

2

Rely on Experts for Pen testing, Not on Pretenders

Humans gravitate to the familiar and comfortable. Some pen testers draw from the same bag of tricks rather than methodically targeting the entire, probable spectrum of risks. Many enterprises have struggled to tell experts from pretenders.

PRO-TIP

Make use of threat frameworks such as Mitre Att@ck. Threat Intelligence providers ought to be selected in part on how well they can narrow focus from the possible to the probable. Avoid using the same pen test firm unless you are certain it is awesome. The difference between two different pen testers can be stark, with one recognizing gaps others missed.

3

Build a Persona Based Cyber Training Program

Effective employee cyber readiness training mitigates major risks. Giving the same training to a receptionist and an IT Systems Admin might be worse than none. Their perceptions of risks (too low) and mitigations (too high) vary greatly. Binge training is soon forgotten, and temporary bumps in vigilance fall back to carelessness. Human problems require human solutions.

PRO-TIP

Individualize employee cyber readiness training. Mine data, through phish simulations and other tactics, to discover higher-risk employees. Use content tailored to different personas. Make readiness a continuous endeavor that instructs, motivates, and reinforces.

4

Make Employees Detection Sensors

Non-IT employees see symptoms of “Miscellaneous Errors” and sometimes intrusions but don’t report them or recognize what they could.

PRO-TIP

Use cyber readiness training to inform them of a class of problems they can identify. Tell them how to report malicious activities periodically. Leverage data analytics to learn what ‘neighborhoods’ users observe. Teach them a few things to ‘detect’. Start small, add gradually. Measure and adapt. Reward discoveries!!

5

Fix Employee False Negatives

Phish simulation inferences struggle to distinguish between recognition and inaction. Employees assume ‘tools’ or others will do what needs to be done. Attacks and vulnerability symptoms dwell longer without assistance from employees.

PRO-TIP

Phish and other simulations ought to measure failures to report. Nobody should feel like they will get in trouble for speaking up. Human issues like these require human solutions. Firms are hiring psychologists to manage this effectively with attrition and unrealized productivity. People-solutions often work better than technology for people-problems.

6

Don’t Patch, Mitigate

On average, it takes 16 days for an enterprise to implement a critical patch and 151 days to patch medium/low ones. Some patches fail to implement properly (e.g., missing file/reference). Some exploit pre-date patches. The value of anti-exploit tools is highly questionable. Behavior analytics tools rely on statistical guesses; many deployments insert a human-in-the-loop to counter false positives, leaving a window of exploitation for the adversary.

PRO-TIP

Implement post-execution controls to limit what high-risk applications can do after they are hijacked, whether due to a missing or failed patch, weaponized document, SQL injection, etc. The adaptiveness of such controls is critical to avoiding a policy quagmire. Look for tools that address all your high-risk applications. The human element here stems from potentially having to communicate with end-users about their workflows to determine what utilities they need or not.

7

Reduce the Attack Surface

Operating systems include dozens of utilities that attackers use in ‘living off the land’ attacks. Disabling some adversely affects nothing, others can be crippling to workflows. Gartner’s magic quadrant for endpoint protection in August 2019, criticized the lack of hardening, which results in increased alerts monitoring, investigation, and response volumes.

PRO-TIP

Disable high-risk utilities. Use controls that accommodate IT/Sec-Ops workflows to utilize them on-demand while denying or restricting end-user and adversary use. Watch out for OS controls that can be disabled by any privileged user or process.

8

Multi-Factor Authentication: Short & Long Term

Not all identified best practices are beyond reach this quarter, such as Public Key Infrastructure (PKI) - based hardware devices to counter password-only weaknesses. And not everybody can quickly jettison legacy protocols, such as NTLM, that expose enterprises to pass-the-hash attacks and more. Yet, credentials are stolen every day.

PRO-TIP

Systems from Microsoft and other vendors include 'other' factors, such as geo-location, host identity, device type, browser tagging, time-of-day, etc. Prioritize your systems and make use of the capabilities ASAP. These certainly do not eliminate risk, but they do reduce it.

9

Pen Test: Turn-Up the Volume

A large enterprise has many layers of detection involving many tools relying on many personnel. Many organizations either do not know how well they use these tools or what they do not detect.

PRO-TIP

For roughly 10% to 30% more in cost, and for one or more days, pen testers can vary the 'noise' they make so cyber defenders can exercise their tools, workflows, and knowledge. Evaluate pen testers on their portfolio of exercises and their ability to distinguish between the possible and the probable. Cyber defenders should be able to relate their observations with representations of what the pentesters did and when they did so.

10

Script Walkthroughs and Full-Dress Rehearsals

The effectiveness of sophisticated cyber defenses is limited by the comprehension and proficiency of the people using these tools within multi-team workflows. During many inadequate responses to incidents, personnel frantically read their IR Handbook and tool user guides. Familiarity with attacker tactics, techniques, and underlying mitigation strategies will make cyber defenders more effective.

PRO-TIP

"Table-top exercises" and "Cyber Wargaming" can transform cyber defenders into an elite team. Special off-enterprise environments hosted by professional services contractors allow for exercises too risky for production environments. But, these do not acquaint defenders with the nuances of their own ecosystem, which is what tends to challenge outsourced analysts. In-house exercises enable personnel to better hone their proficiencies with tools, workflows, and procedures.

Operationalizing workflows dealing with the human element is often compared with herding cats. A prescription optimal for one organization may not be best for others. A crucial point to understand is that cybersecurity challenges are not only about technology and that people-centric remedies are essential. This relates to some NFL teams suddenly becoming contenders with a new coaching staff but essentially the same roster.