More Security Without Spending More Money

There are many security vendors that offer many security features, services, enhancements, and consultations which makes any security budget a very finite resource. It is to that end which has provided the desire to articulate the thoughts in this article. There are many ways an organization can increase their security posture without spending money or by spending rather small amounts that are already (hopefully) included in the budget. This article begins with discussing changes within the domain of people to include personnel, third parties, and customers. Then processes are discussed with technology being the final section. To conclude the final summary the key points will be mentioned for emphasis.

Until AI takes over the world people are needed to to perform work and keep organizations running. The people that keep the organization running consist of employees, third parties such as contractors and service providers, as well as customers. Each type of person brings its own security challenges and has its own set of requirements, employees present unparalleled levels of insider access, third parties can create extreme damage with little risk to themselves, and customers have low interest in identifying and rectifying issues with little ability to differentiate between good and malicious.

> When discussing increasing security protections against insiders such as employees on a diminished or non-existent budget the main talking point should be training and reporting. To be more specific, all (or nearly all) employees should have email addresses, the majority should have a phone, and some should even have access to the physical locations where data systems reside. A great way to train employees is to provide realistic situations that require employees to practice the skills that supposed to be consumed by the training. Practically speaking, the security department (after authorization) could create a public email account (Gmail, Hotmail, MSN, Mail.RU, ect.) with a username that is similar to an employee's (maybe an executive's), craft a very simple email requesting some piece of information (maybe the phone number for some internal department), then send that email to a number of employees. Everyone whom responds to the emails is required to attend additional training. Another practical example would be creating a script that can be read as a security employee calls a number of employees in a vishing exercise. Every employee that provides information requested when called is required to attend additional training. For personnel that have physical access to data resources, piggy-backing and tailgating exercises should be performed to identify if people are being permitted entrance to the building in an unauthorized manner.
>
> Third parties present near the same risk as direct employees without the same level of personal risk. This means that third parties rarely have the same level of interest in protecting organizational assets; therefore, when there is no budget to increase security around third parties contracts and service level agreements should be reviewed. These documents typically should be reviewed annually but that is commonly not performed; therefore, when the budget is finite and workloads are light ensuring contracts, agreements, memorandums, and other documents contain relevant, updated, and explicit language that is unambiguous, clearly delineates responsibilities, and conforms to security and privacy best practices and compliance

requirements is essential. As a reminder, this document is not legal advice and a lawyer should be consulted for any organization's specific or particular needs or circumstances.

Customers present a risk to organizations that is not always appreciated or known but is increasingly becoming a matter that is receiving public attention. Two risks that materialize are password reuse and common password use. Password reuse can be curbed by maintaining a password hash history for a customer. Typical history lengths range from 10 to 18 previous password hashes. When a user attempts to change a password the hash is compared to the historical hashes prior to being permitted as a change. Many provider have this ability 'baked into' their service and just need to have it 'turned on'. Depending on the number of users this could require adding storage to the password database. Common password use can be stopped (or curbed) by using a forbidden password lists. When the user attempts to use a password from the list the password is rejected and the customer must enter a unique password. This solution is also provided with a great number of password management systems and usually requires no additional storage. The forbidden password list often time contains a list of the most commonly used organizational and industry passwords.

It is rare to find an organization where the processes were developed with the intent of maximizing security first and performing the mission of the organization second; thus, it is quite reasonable to believe the majority of internal processes have room to enhance security. As every organization has a unique (or moderately unique) mission and strategy it would be impossible to write a comprehensive document on how to addresses every process. Instead, the processes that will be covered here are compliance to policies and standards, uniformity of coverage, and simplicity with low coupling.

Policies and standards are (or should be) the base of all processes. As such, it is imperative to create a process that verifies policies and standards are updated, consistent with current procedures and needs, as well as relevant to the current operating environment. During this process of reviewing the current set of documentation should be compared against what is actually being performed in the environment. A draft document should be created with updates that reflect the deltas between what is actually happening and what was contained within the policies and standards. The draft must be reviewed by legal and other stakeholders to determine if any updates are outside the realm of being permitted. Once the documents are approved they should be disseminated (this the changes explicitly indicated) to operating procedures can be updated to match.

When policies and standards are disseminated it is not uncommon for exception to be made, personnel to ignore unenforced documentation, or personnel to be unaware of relevant policies and/or standards. For these reasons, it is important to ensure a process to measure the uniformity of coverage for policies and standards. All relevant organizational areas should receive a short questionnaire for each employee that asks which policy or standard a given scenario is applicable and what the consequences for noncompliance may be. An example is having an item that asks an employee which policy requires the user to not share his/her password and what the consequences for doing so may include.

If people are expected to adhere to policies and standards they should be able to understand the policies and standards as well as which policy or standard is relevant. To create simplicity within the documents all jargon and legalize should be replaced with simplistic (plain) language where possible and followed by plain language where legalize is required. Simplicity also requires a fine balance between having one overarching document and many short single-focus

documents. This balance is known as low documentation coupling. The intent of low documentation coupling is to have documentation that corresponds to a single purpose without overlapping with any other documentation. When delineating the areas of responsibility for documentation the first time this can become quite intricate. An example is the creation and use of passwords. Some organizations will have this documented in an acceptable use policy, a password policy, and an accounts management policy and each policy may be worded slightly different with disparate requirements. This overlap and disparity should be removed with a single entry in a single document that defines password creation and use. Even the administrative creation of initial account passwords should be made publicly available with the same password requirements documentation everyone else uses. This will create transparency for users while encouraging administrators are following good security practices.

There is rarely found an organization that does not leverage digital technology. Within all of the organizations that use digital technology for support, there has arisen some commonly used technology vendors and providers. Despite the limited number of vendors that are widely used this document will focus on a few vendor agnostic recommendations and a limited number of vendor specific recommendations that are (or should be) of low budgetary cost for organizations that typically have moderate to good security practices.

All software leads to patching. Although patching is not a new concept it is still one that regularly is neglected for a wide range of reasons that include legacy hardware and software, inconsistent patch enforcement, and bring-your-own-device scenarios. When it comes to legacy hardware and software the best idea is to upgrade or migrate. As those often times require an investment this document will instead offer a low(er)-cost alternative. The recommendation to increase security of these legacy systems is to isolate them within their own vlan that has connectivity restricted to a single “jump box”. A jump box just being an intermediate system that does offer current security, patching, authentication, and intrusion prevention. The jump box should be able to be provisioned using current licenses (or without a license) and may only require an intrusion prevention license (such as an EDR or Network IPS endpoint agent). Patching should be enforced consistently across all enterprise devices without regard to device type. There are a number of network vendor providers that can be provisioned to only permit operating systems to connect only if they are at current patch and version levels. This should be configured for all end-user operating systems to include smart phones, desktops, laptops, tablets, etc. All servers, security devices, NASs, SANs, and other static hardware should be integrated in the corporate patch management system. Patches should include firmware patches as well. All patches should be enforced as well with explicitly defined cut-off dates. If a cut-off date is reached without a system being patched or receiving a waiver the system should be removed from network connectivity until it has been patched and the patch has been verified. In bring-your-own-device scenarios users can bring-their-own-malware which presents a set of concerns that should be mitigated. The majority of these solutions cost money but using the same security mechanisms mentioned above, devices that are not patched, updated, have updated antivirus, and which are not rooted or jail-broken can join the network. If a device does not meet the security policy it should be prevented from connecting.

Identity management is another technical area of great publicity in the security industry that has been made more important with the migration towards zero-trust architectures; therefore, ensuring identities are being used by legitimate entities is paramount. The first area for considerations is to ensure that all systems use a single identity provider. This is often

accomplished using a federated service or password hash sync that is native to most providers and vendors. In the event a solution does not have integration capabilities a feature request should be made (free) or the solution should replaced (can be costly). Once all of the organization's solutions have been integrated (or in parallel with the integration) into a single identity provider multi-factor authentication should be utilized for all human-facing accounts. This should be a requirement for using the information systems for all users without regard to department, managerial or executive level, or personnel type (contractor v. employee). For identities that are not human-facing (service, script, process specific) accounts an extensively long and complex password (recommendation of 99 characters) should be used and rotated annually. The only exception to the annual rotation of service account passwords is the recommendation to rotate the KRBTGT secret in Microsoft AD monthly. This can be accomplished by a Microsoft provided script on Microsoft's site. For human-facing accounts, no complexity requirements should be enforced with a minimum of 16 characters for accounts that are leveraging multi-factor authentication. For human-facing accounts that do not have multi-factor authentication complexity compliance should be enforced with a minimum of 15 characters. As a final recommendation for this identity management section the bad-password count reset timer should be set to no less than 60 minutes. In Microsoft products the default is 15 minutes. This setting is how long it takes the identity provider to reset the number of failed logon attempts to zero after unsuccessful logons. For example, say Employee enters the incorrect password 5 times in a row, the default in Microsoft resets this number to zero after fifteen minutes. The recommendation is to change this wait period to a minimum of one hour to prevent advanced password attacks. Be careful with this recommendation as it may cause account lockouts if the organization is experiencing a password attack.

The final recommendation is to ensure encryption is used everywhere. Ensure all services and APIs are using their most secure configurations and settings. Ensure all databases, storage, servers, mobile devices, tablets, and workstations are encrypted. Ensure all websites enforce HTTPS Everywhere (to force HTTPS with HSTS). Ensure backups are encrypted and stored offline. Ensure all protocols used are encrypted with the latest stable encryption and that all legacy, broken, or outdated encryption in removed where possible and disabled by technical policy where it cannot be removed. Ensure that container registries are encrypted.

This document was intended to provide some recommendations to enrich organizational security without increasing the security budget. There are many way to increase security that have not been covered within this document because they require significant cost, are highly technical (incurring significant cost in time), or make assumptions about preexisting security infrastructure within organizations. This document covered to increase the security to help lower the risk associated with humans, increase the security of and through processes, and concluded with some ways to increase technical security. Every organization has budgetary constraints but few organizations perform all the recommendations mentioned in this article so this might a good review when the purse strings are pinched.

Thank you for reading

-Andrew Kosakowski

www.Anthko.com