Cybersecurity

Tim's List

1. Disaster Recovery planning
    a. It's not a matter of if but when.
        i. Media relations preparedness. A general statement if the breach is made known before you're ready. A carefully worded statement or report if you're releasing the information on the breach on your own terms.
    b. Make a plan and make it diverse for several different types of scenarios
    c. Table-top exercises with IT staff
    d. Be aware of your infrastructure both local and cloud and how they can all interact with each other in any way
    e. Backups!
        ii. 3, 2, 1 is still a good method to follow
        iii. Depending on the type of data and how critical it is. Schedule backups daily, weekly, bi-weekly, monthly, quarterly, bi-annually and annually.
        iv. Check your backups frequently to verify the data
        v. Schedule backup restore testing semi-frequently, bi-annually and/or quarterly
    f. Fail-over/redundancy
        vi. If possible, have a secondary location or method for server/networking fail-over
        vii. Test your fail-over process semi-frequently, bi-annually and/or quarterly
        viii.
2. A/V
    g. A/V monitoring and alerts when a device is or has been compromised
    h. An open group chat with your IT department heads and/or other applicable staff to quickly discuss the nature of what's happening when an alert comes in.
        i. Helps to diversify the load of checking network/data integrity as quickly as possible.
    i. Enhancements to A/V
        ii. AppLocker
        iii. Powershell security measures (I.e. what was mentioned in 9/29 webcast)
    j. Ability to quickly isolate a device, devices or entire location(s)
        iv. Pre-built "kill switch" whether built-in or custom built which can kill one, multiple or all network connections.
        v. Goal being to stop the spread
3. Pen Testing
    k. Multiple Vendors - i.e. one specific vendor one year, a different vendor the following year.
    l. Self-pen testing/auditing - ties in with reporting
4. Reporting!!!
    m. PDQ Inventory reporting on endpoints
        i. Software – Microsoft apps, third-party software...
        ii. Hardware – driver/firmware updates

n. PDQ Deploy for scheduled deployment of Powershell-based or other types of scripted reports
o. Custom reporting for Active Directory – Powershell, Qradar...
    iii. User access – via direct access to folders, PCs, servers or via security groups
    iv. ACLs for built-in security groups, new/elevated (greater access) security groups, service accounts, OUs...
    v. Security Group monitoring/reporting - for current accounts/groups and/or new additions/subtractions made on a daily, weekly or monthly basis
p. User offboarding
    vi. Verifying accounts are disabled/deleted and/or access removed that is no longer necessary and done in a timely manner.
    vii. Malicious IT and/or staff separation
        1. Verify any/all AD, AAD and any other misc "cloud" accounts belong to an actual person and not a dummy account
q. eDiscovery
    viii. Ensure you have a method for eDiscovery, should you desire it or if it is required for your organizations type of work.

5. Conditional Access
    r. Either local, cloud or ideally both
    s. Prevent connections for specific staff or from specific locations/countries to internal and/or cloud resources
6. Staff/user training.
    t. Setting required deadline(s) for completing training modules
    u. For IT staff, similar as well as enhanced training
        i. Since IT staff "hold the keys to the kingdom" additional training is good to ensure those staff are aware of the "power" they hold
7. Patch Management/Notification
    v. Microsoft (Windows/Office or other installed Microsoft products)
    w. Third-party (Adobe, Chrome, WinSCP...)
    x. 0-day monitoring and rapid testing for deployment to mitigate endpoints
        i. VMs for rapid testing and/or for monthly, regular patch testing
    y. Using a "ringed" approach
        ii. Ring 0 – Small group of testing machines. Not for production use.
        iii. Ring 1 – SME testing workstations. Not production use
        iv. Ring 2 – Small group/division of production machines
        v. Ring 3, 4, 5...
    z. A regular update schedule for both Microsoft and third-party apps
    aa. Setting/allowing auto-updates where available and if they are applicable
    bb. Sign-up for alert notices and/or manual searching from software vendors, US-CERT, CISA, popular blog/forum pages (bleepingcomputer)
8. MFA
    cc. MFA for everyone! Especially those granted access to cloud resources (i.e. Outlook, OneDrive, G Suite...), IT with any degree of elevated access and/or "high profile" staff
    dd. MFA for VPN solution(s)

ee. MFA and conditional access working together – not only something you have and something you know but also geolocation and/or device AD/AAD joined.

9. Password management
    ff. Policies: length, complexity, diverse between separate login types/places, expiration/enforced changing
    gg. Reporting, where applicable
    hh. Enforced by tech, such as GPO or other policy mechanisms or written policy which is agreed upon by staff at time of employment or ratified/updated by management.
10. Network monitoring/blocking
    ii. Using at least a couple pieces of software and/or tools to be able to audit and monitor internet traffic in, out and between your intranet and the internet
    jj. Having a Firewall in place for access control and to prevent staff from reaching certain websites which are not necessary for work purposes (i.e. blocked file sharing sites, instant messaging platforms, pornography and/or other taboo/known malicious sites...)
    kk. Network Access Control – allowing certain or approved devices access to network resources but blocking unknown devices or devices not meeting certain criteria
        i. Criteria could be personal devices or devices not meeting a certain level of software updates as examples
11. Social engineering
    ll. Be aware of not only websites or emails with malicious intent but also “rogue” hardware.
        i. Such as “found” or “presented” USB devices or lesser-known manufacturers of IT peripherals.
    mm. Verify credentials of third-party support vendors coming on-site or providing remote access.
        ii. If possible request/require background checks
    nn. Be careful and aware of work-related photos posted to social media
        iii. May contain sensitive information in the background