Secure Guard Consulting | (515) 229-5674 | kkothari@sgcsecure.com | www.secureguardconsulting.com

Secure Guard Consulting LLC – *www.secureguardconsulting.com*

Secure Guard Consulting performs full-service cybersecurity/IT auditing and consulting. This includes internal security assessments, external security assessments and external penetration testing, IT general controls reviews, and social engineering (phishing, phone, in-person). The company was founded in 2012 by Kaushal Kothari, a certified ethical hacker and former FDIC IT examination analyst.

CONTACT:

Kaushal Kothari
Secure Guard Consulting
180 Aidan Street, Waukee IA 50263
Phone: 515-229-5674 / Email: *kkothari@sgcsecure.com*

ABOUT SECURE GUARD CONSULTING

MICROSOFT 365

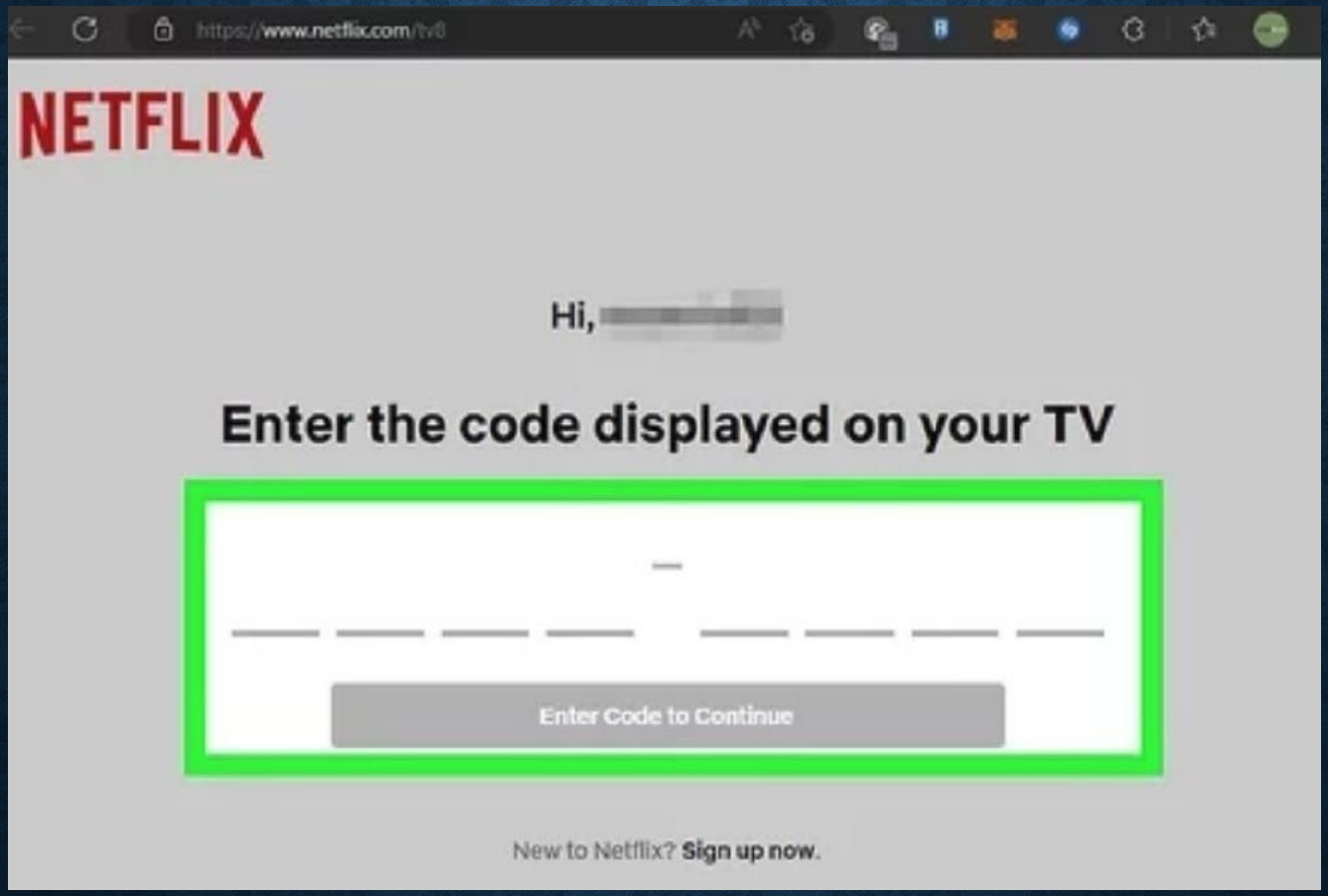
Critical Hardening Steps!

(515) 229-5674 kkothari@sgcsecure.com

GLOBAL ADMIN

- Similar to the network, ensure global admin accounts are separate and cloud-only, as privileged access should not be assigned to an individual's normal user account (e.g., create an admin.jdoe@company.onmicrosoft.com account and assign it global admin privileges). Note: Make sure to sign in and get MFA established on the new global admin account and remove global admin capability from the normal user account.

(515) 229-5674 kkothari@sgcsecure.com



(515) 229-5674 kkothari@sgcsecure.com

DEVICE AUTH

- Codes can be used to authenticate another session
- Input the code in a browser where you are already authenticated
- Victims are phished to input a code we control
- As the victim is already authenticated in their browser conditional access policies and MFA are satisfied
- Block authentication flows (device auth). Conditional access policies are required in order to accomplish this, so licensing changes may be necessary. Alternatively, if 365 logging and monitoring is in place, obtain real time alerts of any authentication flows created and investigate accordingly. See https://learn.microsoft.com/en-us/entra/identity/conditional-access/how-to-policy-authentication-flows for more details.

(515) 229-5674 kkothari@sgcsecure.com

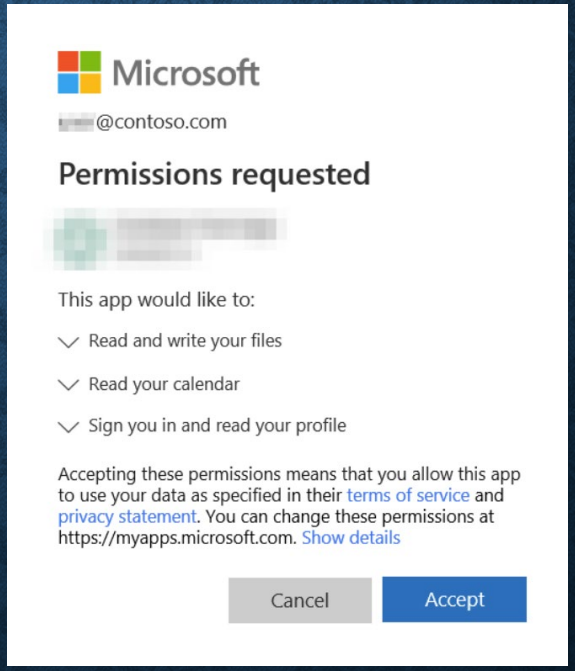
USER CONSENT

- Applications can be built to be "multi-tenant"
- Various permissions can be set for the apps in relation to the user's account
- For example an app can be set to have permissions to read a user's email or profile
- The user receives a link to a login.microsoftonline.com page
- Then a consent page is displayed

(515) 229-5674 kkothari@sgcsecure.com

USER CONSENT

- If the user accepts, the application now has the set permissions on the target user account



(515) 229-5674 kkothari@sgcsecure.com

USER CONSENT

- Block user consent. Alternatively, if 365 logging and monitoring is in place, obtain real time alerts of any user consent actions taken and investigate accordingly. See https://entra.microsoft.com/#view/Microsoft_AAD_IAM/ConsentPoliciesMenuBlade/~/UserSettings?Microsoft_AAD_IAM_legacyAADRedirect=true for more details.

(515) 229-5674 kkothari@sgcsecure.com

TEAMS PHISHING

- Hacker breaches vendor A.
- Commonly, they can initiate emails from Vendor A, so these would generally be trusted emails, and legitimate because they're being sent actually from them.
- Another avenue though.
  - Hacker opens Teams and sends your bank a message with a phishing link in it.
- Block all external domains to prevent unmanaged external Teams users from starting a conversation with people in the organization (https://admin.teams.microsoft.com/company-wide-settings/external-communications).

(515) 229-5674 kkothari@sgcsecure.com

CALENDAR

- Block ability for users to share their calendars with people outside your organization (https://admin.microsoft.com/?auth_upn=kkothari%40sgcsecure.com&source=applauncher#/Settings/Services/:/Settings/L1/Calendar).

(515) 229-5674 kkothari@sgcsecure.com

EVILGINX

- Evilginx2 - https://www.youtube.com/watch?v=yildvg4FJLU

(515) 229-5674 kkothari@sgcsecure.com

EVILGINX SOLUTION 1

- Block all OWA
- Blocking all email outside of their trusted IPs
- Utilize an MDM solution to manage mobile device enrollment. The bank should manually approve device connection requests.

(515) 229-5674 kkothari@sgcsecure.com

EVILGINX SOLUTION 2 (ENROLL ALL)

- Enroll all devices (laptops, PCs, everything) into Intune. The bank should manually approve device connection requests.

(515) 229-5674 kkothari@sgcsecure.com

EVILGINX SOLUTION (FIDO2)

- FIDO stands for Fast Identity Online
- FIDO device and application create a cryptographical link.
- The FIDO device creates this link based on the site/application domain name.
- Each site is given a Relying Party ID (RPID).
- Historically to use FIDO2 we need an external device. (Yubikey)

(515) 229-5674 kkothari@sgcsecure.com

EVILGINX SOLUTION (PASSKEYS)

- This is where Passkeys come in.
- Passkeys utilize the FIDO2 standard for authentication.
- Keys are store securely in cloud service
  - Google account • iCloud Keychain • Microsoft Authenticator (Public Preview)
- https://www.youtube.com/watch?v=wTLB0Yh70_0

(515) 229-5674 kkothari@sgcsecure.com

SIEM / RISKY BEHAVIOR

- SIEM should look at where the MFA authentication was actually occurring and compare it to where the authenticated session was created. This should be blocked when suspicious.
- We've heard Microsoft's risky logins can block this attack, but we haven't tested it.

(515) 229-5674 kkothari@sgcsecure.com

SOFT PROTECTIONS

- Train users annually, if not more, that when they go to type in their MFA codes, that they look at the URL closely to make sure it's truly the intended site.
- Block, via web content filtering, newly created domains (this won't get everything, but should capture some attacks).

(515) 229-5674 kkothari@sgcsecure.com

MOMMY WHERE DO PASSWORDS COME FROM?

- In 1961, Fernando Corbato who was an MIT professor had a problem.
- He needed to give multiple users private access to the same system.
- His solution?
  - The 1st implementation of the digital password.
  - His solution has been our problem ever since.
- To the future – MFA – pretty good.
  - Microsoft says it protects against 99% of attacks.
- But, it doesn't do all. – enter FIDO2
- And some day, hackers will figure out FIDO2 and a new solution will be needed.

(515) 229-5674 kkothari@sgcsecure.com

WE STILL NEED MFA

Implementing MFA across the user base isn't enough – you have to make sure the user goes out and signs in and gets MFA in place.

*****Conditional Policies – Conditional Policies - Conditional Policies – Spend the Money Now or Spend it Later.*****

Always Trust But Verify!

(515) 229-5674 kkothari@sgcsecure.com

CONDITIONAL ACCESS POLICY NOTE

- If you're using conditional access policies to manage MFA, it's important to disable legacy "per user MFA" – can do it in bulk or individually.
- Microsoft gets confused!

(515) 229-5674 kkothari@sgcsecure.com

ADDITIONAL HARDENING

(515) 229-5674 kkothari@sgcsecure.com

SHARED MAILBOXES

- Shared mailboxes don't take up licenses.
- Should assign access rights to the shared account as opposed to using a shared password / credentials (assigning shared mailbox access).
- A password is created by default, so ensure sign-in to shared mailboxes is blocked.

(515) 229-5674 kkothari@sgcsecure.com

EXTERNAL FORWARDING RULES

- Ensure external forwarding rules are disabled.
    1. Navigate to https://security.microsoft.com
    2. Select Email and Collaboration
    3. Policies and Rules
    4. Threat Policies, Anti-spam Policies
    5. Select Anti-spam outbound policy (Default) and change Forwarding Rules to 'Off – Forwarding is disabled')
- This can restrict email from being forwarded to an outside.
- Limited exceptions should be made for distribution or administrative accounts for IT providers.

(515) 229-5674 kkothari@sgcsecure.com

AUDIT LOGGING

- Enable audit and mailbox logging.
- Ideally, have log files shipped to a SIEM or similar solution for analysis.
- At this point, if your logs aren't being shipped to someone for analysis (e.g., SIEM), you are at risk.

(515) 229-5674 kkothari@sgcsecure.com

LEGACY AUTHENTICATION

- Disable Legacy authentication

(515) 229-5674 kkothari@sgcsecure.com

MOBILE DEVICES

- Use an MDM solution.
  - Microsoft Intune
  - IBM MaaS360
- ActiveSync – Retired – So without MDM, remote wipe capability does not appear to be available any longer.

(515) 229-5674 kkothari@sgcsecure.com

EMAIL DOMAIN HEALTH

- Ensure email/domain health is in good standing
  - https://mxtoolbox.com/emailhealth
  - Focus on Errors

(515) 229-5674 kkothari@sgcsecure.com

IDENTITY PROTECTION

- Block app registrations (https://www.trendmicro.com/cloudoneconformity/knowledge-base/azure/ActiveDirectory/users-can-register-applications.html).

(515) 229-5674 kkothari@sgcsecure.com

IDENTITY PROTECTION

- Ensure user consent to apps accessing company data on their behalf is not allowed
- Ensure the admin consent workflow is enabled
    1. Navigate to Microsoft Entra admin center https://entra.microsoft.com/.
    2. Click to expand Identity > Applications select Enterprise applications.
    3. Under Security select Consent and permissions.
    4. Under Manage select Admin consent settings.
    5. Set Users can request admin consent to apps they are unable to consent to Yes under Admin consent requests.
    6. Under the Reviewers choose the Roles and Groups that will review user generated app consent requests.
    7. Set Selected users will receive email notifications for requests to Yes
    8. Select Save at the top of the window.

(515) 229-5674 kkothari@sgcsecure.com

B2B COLLABORATION

- A simple invitation and redemption process lets partners use their own credentials to access your company's resources (https://learn.microsoft.com/en-us/entra/external-id/what-is-b2b).
- Ensure that collaboration invitations are sent to allowed domains only, or restrict to only your own domain (https://learn.microsoft.com/en-us/entra/external-id/allow-deny-list).

(515) 229-5674 kkothari@sgcsecure.com

- Ensure conditional access are blocking unapproved geographical locations.

(515) 229-5674 kkothari@sgcsecure.com

REQUIRES HIGHER LICENSING

- Ensure a custom banned password list is in place containing company name.
    1. Navigate to Microsoft Entra admin center https://entra.microsoft.com/
    2. Click to expand Protection > Authentication methods
    3. Select Password protection
    4. Verify Enforce custom list is set to Yes
    5. Verify Custom banned password list contains entries specific to the organization, or matches a pre-determined list.
- Brand names • Product names • Locations, such as company headquarters • Company-specific internal terms • Abbreviations that have specific company meaning

(515) 229-5674 kkothari@sgcsecure.com