SUBGRAPH

Prepared for: ASL19

Subgraph Technologies, Inc.
642 rue de Courcelle, Suite 309
Montreal, Quebec
https://subgraph.com

Overview and Methodology

The base methodology for this audit is the SAFETAG framework (https://safetag.org):

https://github.com/OpenInternet/SAFETAG/releases/download/v0.4/SAFETAG.Full.guide.English.pdf

The actual audit used SAFETAG as a base-line and was further customized by Subgraph to fit the organizational characteristics of ASL19.

To conduct the audit, we performed the following activities with the help of ASL19:

- Interview with key staff
- Technology inventory
- Data inventory
- Key process identification
- Review of policy documents and training material
- On-site network security scan
- Facility tour and physical security review
- Remote application scan
- Open source intelligence review

The audit is structured into a number of separate domains. The domains covered included:

- Organizational and threat context
- Capacity assessment
- Reconnaissance
- Network security
- User device assessment
- Data
- Application security
- Cloud security
- Credentials and privileged users
- Organizational processes
- Communications and operations security

Most activities during this audit were conducted during the month of June 2017. The on-site visit was June 22-23.

Findings Summary

No.	Finding	Severity
V-001	Unrestricted physical access to LAN	Low
V-002	Infrequent/ad-hoc rotation of wireless password	Low
V-003	Recognizable SSIDs	Low
V-004	Handling of shared passwords	Low
V-005	Handling of PGP keys used by staff	Low
V-006	Critical non-OS software updates not applied automatically	Medium
V-007	Dormant shared files	Low
V-008	Limited control over OAuth grants by users	Low
V-009	Use of cloud apps without multi-factor authentication	Low
V-010	Custodianship of app signing key	Medium
V-011	Risk of vulnerable third-party software components	Low
V-012	No integrated software security testing	Low
V-013	Use of credentials in code	Low
V-014	Shared developer credentials	Low
V-015	Redacted finding	Medium
V-016	Redacted finding	Medium

Introduction and context

ASL19 is an organization that is primarily focused on helping Iranians access the Internet without restrictions. [[Redacted specific organizational details]].

Key Processes

Software development

ASL19 is primarily a software development shop. They produce and help distribute applications that assist individuals in Iran with circumvention of nation-spanning Internet censorship. All software development is done in-house by ASL19 staff members who comprise about half of the total ASL19 staff. Graphic design work is also done in-house by ASL19 staff.

Research

ASL19 has a team of researchers who are contractors led by full-time staff members. The researchers are primarily responsible for monitoring political events in Iran and creating content for certain ASL19 projects, such as the RouhaniMeter and FactNameh.

Outreach

ASL19 has dedicated staff for outreach, including social media communications via Twitter, Facebook, and Telegram.

Management

Finance and HR are both managed in-house to minimize the exposure of *personally identifiable information* (PII) to outsourced third-parties. The finance team, for example, is compromised of three individuals. Key processes for this team include:

- Hiring, on-boarding, off-boarding
- Payroll
- Bookkeeping
- Tax

ASL19 also shares project management among a team of three, with one full-time staff member responsible for managing relationships with funders.

Data Summary

The data of highest sensitivity at ASL19 is the collection of identities of organization staff. Most ASL19 staff use pseudonyms because of the risk of harassment and threats to personal security. [[Redacted specific threat detail]].

Other data that also needs to be protected includes:

- Very limited user registration data for various apps and services offered by ASL19
- Funding and contract details
- Data encryption keys
- Credentials for online services
- Application signing keys
- Address of office

Adversary profile

ASL19 is a potential target of state level threats who may wish to:

- Disrupt their operations
- Undermine trust in the organization
- Discover the identity of organization staff (for harassment/intimidation)
- Impersonate organization staff
- Discover the identity of users

The threat source has, in the past, demonstrated capability to:

- Attempt social engineering/phishing against ASL19 staff
- Perform attacks against web applications

ASL19 staff have experienced phishing attempts. They have also been harassed by unknown actors contacting them from the Internet and, in one case, telephone. In at least one instance a hostile individual attempted to persuade an ASL19 staff member to open a malicious file sent by email.

[[Redacted specific threat detail]].

Capacity profile

ASL19 has a fairly security-savvy IT management team comprised of three staff members. The growth of capacity to support these controls is fairly recent, and as a result, many key controls are still the responsibility of a single person. This results in process bottlenecks, particularly where some processes require physical proximity.

ASL19 has developed policies/procedures for:

- General security, which must be signed by all staff
- Onboarding
- Travel

ASL19 also has recently begun implementing quarterly organizational security review process. This process covers:

- Changing wireless passwords
- Reviewing online back-up
- Reviewing security policy
- Reviewing hosted shares
- Reviewing staff security posture with respect to on-boarding procedures

ASL19 security policies are to be reviewed and updated annually.

Asset Management

Laptops

ASL19 staff are provisioned laptops as primary workstations. These laptops are hardened by one of the ASL19 security administrators prior to delivery to staff. With the exception of the development staff, users are not allowed to have administrative access to their laptops. Hardening includes:

- Enabling full-disk encryption
- Enabling the firewall
- Installing Chrome and setting it as the default browser
- Disabling the password manager for Google Chrome
- Installing privacy/adblock browser extensions
- Setting the desktop screenlock timeout to a short value
- Installing security tools: password manager

Most staff do not take their laptops home. One management gap related to user endpoint devices is a general inability to perform remote administration. Administrative tasks, such as manual upgrades/patch installation, must be done by staff on-site.

Desktops

HR and Payroll data is stored on computers that do not ever leave the office; this is because of the data sensitivity. Two sensitive desktop computer systems at ASL19 are not connected at all to the Internet for the purpose of preventing unauthorized access to data. [[Redacted further detail]].

Phones

ASL19 staff are provisioned phones with centralized device management to control installation of apps. [[Redacted further detail]].

Mobile users always access the Internet using a *VPN*. *VPN* access is sourced by a commercial provider. Each ASL19 staff member has their own account with the provider.

Portable storage media

USB storage media are not commonly used at ASL19. They are used on occasion when data needs to be physically moved. There is no encryption used for the devices themselves in these cases (which usually involve encrypted *PGP* or *SSH* keys that need to be shared). USB drives are generally not provided to staff.

Recommendation

Subgraph recommends using encryption for USB drives. [[Redacted specific detail]].

Evaluation of new solutions

Technologists at ASL19 will evaluate the security of all new technology solutions employed by staff. Considerations include:

- Open source
- Endpoint encryption / local management of keys

One example of these considerations being applied to a provisioning decision was in the selection of their endpoint backup solution. Based on the criteria above, the solution they selected performs encryption locally before cloud storage, with all keys managed and stored locally.

Communications provider

[[Redacted detail]].

As a security precaution, ASL19 has registered additional security questions with the provider. This security measure is to mitigate the risk of social engineering and identity impersonation attacks against the provider. Any changes to office Internet connectivity must be authenticated with additional scrutiny setup by ASL19 management. [[Redacted further detail]].

Recommendation

[[Redacted]].

Network security

Most work is done on ASL19 owned laptops within the office. There is very little in place in the way of local collaboration facilities accessible or hosted internally. Most data is stored on cloud infrastructure, and is served over *HTTPS* and requires *multi-factor authentication*.

Internal / external office network scan

A full port scan was conducted of the */24* CIDR internal network allocated for office guests. No ASL19 infrastructure was detected as a result of the scan. There were also no listening ports observed on the internal side of the gateway device that could expose router attack surface.

No listening network services were observed during an external scan of the Internet IP address of the main office network.

V-001: Unrestricted physical access to LAN

Discussion

There was no physical restriction to prevent gaining Ethernet access to the office LAN once inside the office. A visitor or intruder could surreptitiously attach a malicious device to the network where it should not be normally possible. The impact is slightly mitigated by the lack of local LAN infrastructure to attack directly once on the network, though other attacks may be possible.

Recommendation

Certain sensitive hardware and computer systems should be in a locked room to prevent tampering. This should also include the office router and other sensitive network gear.

Wireless

The local wireless network is secured with *WPA2* and the password is given only to staff. Guests are provisioned with a password for a separate wireless network. The second ASL19 office has its own wireless network with a distinct *SSID* and *WPA2* password.

V-002: Infrequent/ad-hoc rotation of wireless password

Discussion

Interviews with staff revealed that the passwords for both the staff and guest Wi-Fi networks are changed infrequently, in an ad-hoc manner, with no rotation schedule.

Recommendation

This is slightly mitigated by lack of local infrastructure, however it would probably be beneficial to have an annual rotation of at least the guest Wi-Fi password. Though staff interviews indicated that passwords were changed on an ad-hoc basis, recently created security procedures include a quarterly password wireless password change.

V-003: Recognizable SSIDs

Discussion

All three of the wireless networks have identifiably "Persian" like names, while all other observed surrounding wireless networks did not. Subgraph recommends using an *SSID* that is not immediately identifiable as probably belonging to ASL19. Recognizable *SSIDs* that are detectable within a fairly large physical area can also reveal the precise physical location of the ASL19 premises with great accuracy.

Recommendation

The wireless networks should be renamed to something that isn't recognizable if someone is actively searching. Hidden *SSIDs* are not really a solution except against a very casual searcher. Subgraph recommends using a generic name similar to those provided by default in telco-supplied network hardware.

Privileged users and credential management

Privileged users

There are three staff members with general privileged access. These privileges include:

- Cloud administration [[Redacted specifics]].
- Proximity pass for physical entry
- Internet provider

Additionally, members of the development team have delegated administrative access to the following:

- AWS
- Application infrastructure

Credential management

The use of a centralized cloud collaboration system simplifies the number of credentials most users have to deal with. However, there are some passwords users must still manage. For this, use of a password manager is mandatory. Well-known password managers are used by staff to generate complex passwords and store them.

Shared credentials

There are a few credentials that must be shared among both the administration team and the developers. These include passwords, *PGP* keys, and *SSH* keys. *SSH* keys and *PGP* keys that are shared by developers (for host administration and application signing) are encrypted and transferred physically.

V-004: Shared passwords

Discussion

Certain passwords must be shared, and there is no elegant or safe way to do this currently in place at ASL19. When these passwords need to be changed, new credentials must be communicated among staff members somehow.

Recommendation

[[Redacted detail]]. ASL19 may consider using a shared KeePass database stored at a central shared device. KeePass supports shared access to a password database stored at a remote location. There are multiple likely configurations that could satisfy the requirements of ASL19. The database should also be regularly backed up to mitigate risk of failure of the local network storage service.

See http://keepass.info/help/base/multiuser.html (this also likely applies to KeePass derived tools).

Operations and communications security

Instant messaging

[[Specific detail redacted]]. XMPP + *OTR* are used for instant messaging. Keys are generated by the user when they setup the instant messaging software and are backed up as part of the disk backup process.

Redacted section

[[Section redacted at request of ASL19]].

Email

[[Section related to e-mail redacted at request of ASL19]].

PGP Keys

Keys for encrypted email are generated by the user themselves during their onboarding process. The passphrase on the keys is set by the user, and no back-up is made by ASL19 staff.

V-005: Handling of PGP keys used by staff

Discussion

PGP keys stored on desktop / laptop systems are backed up through the endpoint backup solution used at ASL19, however the private keys are encrypted with a passphrase that is not backed up. Also, not all keys used by staff are signed by other members of ASL19 before they're exported to public keyservers.

Recommendation

ASL19 should consider making a secure back-up of the private key at the time of staff onboarding. This would permit recovery in the case of hardware/backup failure, or if a staff member leaves the organization without providing the passphrase to unlock the private key.

Subgraph also observed that staff *PGP* keys are often not signed by anyone. While the authoritative source for obtaining an ASL19 staff member's key is their staff page, which is served over *HTTPS*, the keys are still sent to public *PGP* keyservers. Because many users default to public keyservers as a source for public keys, Subgraph recommends that ASL19 staff sign each others keys to help mitigate the risk of impersonation on the public keyservers. The willingness of the adversary to impersonate staff should be considered as a reason to do this.

Organizational security

Data classification

There is no formal definition of what is considered sensitive within ASL19. Staff interviews revealed that data sensitivity is part of the culture of the organization, which is plausible given the work they do and the fact that most of them are using pseudonyms.

Hiring and vetting

[[Redacted]]. ASL19 has a non-disclosure agreement (NDA) that all employees and contractors must sign. [[Redacted details]]. ASL19 staff must also sign a security policy.
[[Redacted details]].

Recommendation

[[Redacted]].

Staff on-boarding/off-boarding

The ASL19 security management team has a process for on-boarding new staff, and implementing that process is chiefly the responsibility of a single team member. The steps for on-boarding are well defined, and include:

- Training on passwords and encryption
- Hardening laptop
- Adding to appropriate groups / enabling *multi-factor authentication*
- Creating PGP keys
- Enabling archiving
- Mobile device setup
- Creating web / cloud accounts
- Social media setup
- Setup of IM communications tools

These items are documented in detail in a spreadsheet/checklist.

Off-boarding requires working through the same checklist. Most access to data is immediately revoked through centralized controls: the email address (and login) can be disabled or suspended. ASL19 staff must also sign a security policy.

Recommendation

[[Specific recommendation removed following clarification from ASL19 about their process, which is clearly defined]].

Redacted section

[[Section redacted at request of ASL19]].

Training

ASL19 staff are trained to use:

- Pretty Good Privacy encryption (PGP) / mail client
- XMPP client with Off-the-Record Messaging (OTR)
- Password management tools

ASL19 also receive basic operational security training and guidance for when they travel. ASL19 has regular reminders to staff about the risk of phishing attacks.

Payroll

Employee paycheques / stubs are provided to employees directly in sealed envelopes. The outsourced firm that handles payroll and source deductions for ASL19 has been configured so that users can manage and view information related to their compensation themselves directly, using their own password.

Redacted section

[[Section redacted at request of ASL19]].

Travel

ASL19 has special security procedures for employees who travel.

[[Further detail redacted at request of ASL19]].

Recommendation

[[Further detail redacted at request of ASL19]].

Vulnerability Management

End user systems

ASL19 staff endpoint systems are configured to have mandatory installation of operating system updates. All of staff are configured at onboarding to use the Chrome browser. Certain apps installed on endpoint systems may not be patched automatically.

V-006: Critical non-OS updates not applied automatically

Discussion

Some applications used by ASL19 staff are not upgraded automatically.

[[Redacted specific details]].

Recommendation

ASL19 must be vigilant in maintaining awareness of new security vulnerabilities, and must rapidly patch end-user systems if required to do so. Remote / traveling users presents a challenge, as all patching of non-OS software requires manual intervention by an administrator. As mentioned above, ASL19 should investigate remote access solutions for providing this kind of remote support or provide clear policy and training for what to do in a situation where a user's system cannot be patched.

Awareness of new vulnerabilities

For those vulnerabilities that do not get automatically fixed through operating system and application auto-updates, the security team at ASL19 subscribe to security mailing lists and have their own communications channel for discussing and coordinating a response to new security threats.

Cloud security

Redacted section

[[Redacted section at request of ASL19]].

AWS

AWS is used as a back-end for essentially all applications developed by ASL19. ASL19 uses the following AWS services:

- EC2
- RDS
- DynamoDB
- IAM

Identity and access management

There is only one administrator who holds the credentials for the AWS master account. Lesser privileged administrative accounts have been created with policies defined using IAM. These accounts are used by both the other security responsible staff at AWS as well as the development leads.

All console AWS authentication by users requires *MFA*.

The collaboration cloud master account is also held by only one individual at ASL19. Administrative capabilities have been recently delegated to two other team members.

Compute

For compute capacity, ASL19 is using EC2. ASL19 is not following a pattern where hosts appear and disappear quickly. As a result, security patches must be applied regularly. ASL19 has stated that their staff will log into hosts and apply security patches when required. The *SSH* keys used to do this are shared between the staff members who are responsible for these services.

VPCs and Security Groups

ASL19's application infrastructure is not extremely complicated so complex configurations within AWS are not necessary. ASL19 has begun using virtual private clouds (VPCs) with one application per *VPC*. All ASL19 instances are placed in security groups that restrict ingress communication except to authorized ports.

Redundancy

All ASL19 applications deployed into AWS are hosted in two availability zones to mitigate the risk of AWS outages.

Redacted section

[[Redacted at request of ASL19]].

V-007: Dormant shared files

Discussion

There isn't any strong control over historical documents shared with third parties and remain shared after project completion.

Recommendation

ASL19 should write a script that audits the shared files stored in cloud data stores with a scheduled clean-up access to remove access no longer required.

V-008: Limited control over OAuth grants by users

Discussion

ASL19 has fairly weak control over the *OAuth* authorizations that users can perform with their own ASL19 accounts. Users are currently able to grant 3rd party cloud applications access to various data stores.

Recommendation

ASL19 should monitor for *OAuth* grants made by users. It is likely possible to do programmatically by writing a script that uses the cloud API.

V-009: Use of cloud apps without multi-factor authentication

Discussion

Not all cloud providers used by ASL19 support *multi-factor authentication*.

Recommendation

Passwords for these services should be securely generated and stored in a password management tool. This is the current practice at ASL19.

Software development

Approximately half of the ASL19 team are software developers. ASL19 develops web-based applications, mobile apps, and app backends.

Sensitive data that is collected includes registration information for users of some of their applications.

ASL19 software developers obfuscate sensitive information before storing it in cloud databases. Pentest firm Cure53 recommended increasing resistance to dictionary/brute-force password guessing attacks and these recommendations were implemented.

Redacted section

[[Redacted section at the request of ASL19]].

Source code management

ASL19 uses git and two hosted services for managing source code and distributed development. Github is used only for those repositories intended to be public.

[[Redacted further detail]].

Credential management

Certain applications require sensitive information to be included in the source code repositories.

[[Redacted further detail]].

Redacted section

[[Redacted section at request of ASL19]].

V-010: Custodianship of app signing private key

Discussion

Apps are signed using a signing keypair that is shared between application developers. This key is challenging to change/rotate because of app-store constraints. Once an application is registered with a signing key, there is no way to revoke that key. Consequently, if a developer leaves ASL19, there is a chance that the private key may remain in their possession. Staff interviews revealed that only one developer had left ASL19, but this risk could grow in the future unless addressed strategically.

Recommendation

This is a tricky problem for ASL19 to solve. The private key that is used to sign apps should not be directly handled by developers, if possible. Either a secured build / signing station should be used, with a dedicated custodian (the private key could be on a hardware device, for example, with a backup held in secure physical storage by key staff).

Light vulnerability scan of deployed web-apps

Subgraph performed a light web application vulnerability scan at the request of ASL19 for one of their websites. This was done because of a suspicious scanning event that was detected by ASL19 had occurred where the attacker scanned three unrelated sites in an identical fashion, suggesting that it was targeted rather than random Internet noise. The scans were performed using two open source scanning tools and yielded no serious vulnerabilities.

V-011: Risk of vulnerable third-party software components

Discussion

Management of third-party components is an issue that has led to security vulnerabilities in the past. Back-end components and plug-ins for frameworks do not get tracked or updated except in an ad-hoc manner.

Recommendation

It is difficult to eliminate the use of third-party modules and components when building complex web and mobile apps. Subgraph recommends that some effort be made to standardize on robust platforms and inventory all exceptions so that updates and vulnerabilities can be monitored/tracked. A service / tool for monitoring third-party components may be useful: AppCanary is one such solution (commercial).

[[Redacted detail]].

V-012: No integrated security testing

Discussion

While ASL19 software is almost always pen-tested, security testing is not integrated into the build process.

Recommendation

Secure software development practices at ASL19 could be improved by integrating security testing into CI. A free software tool such as OWASP ZAP could be used to add testing to the build / test process, making vulnerability discovery happen earlier, long before the penetration testing stage is reached. This will also increase the development team's knowledge about secure development and using security tools as part of their dev / testing process.

V-013: Use of credentials in code

Discussion

There wasn't a major risk observed, but the use of cloud credentials by back-end server code could be improved for AWS applications that need to authenticate to other AWS services.

Recommendation

Managing cloud credentials could be improved by taking advantage of instance roles and the security token service made available by AWS. Applications could retrieve temporary credentials from the instance metadata that correspond to the role the instance is launched under.

More information:

http://docs.aws.amazon.com/IAM/latest/UserGuide/id_credentials_temp_use-resources.html

---

V-014: Managing shared credentials

Discussion

Certain credentials related to the software development life-cycle at ASL19 are shared. These include accounts for cloud services and keys used to sign code.

Recommendation

Shared credentials can be stored using a multi-user KeePass database. ASL19 should delegate code-signing responsibilities to specific staff members (to the extent possible), which may vary on a per-app basis.

Environment segregation

ASL19 launches different instances for production and non-production deployments. This is implemented using environment variables provided to Ansible.

Disaster recovery

Most data related to work by ASL19 is stored in the cloud. This is because of their heavy use of hosted services, as well as code. Data stored on physical disks of staff laptops is automatically backed up to the cloud after being encrypted locally.

A small number of disaster recovery blind spots were uncovered during the audit:

1. The cloud-based backup solution they use backs up disk contents. The use of some encrypted volumes and encrypted credentials (such as *PGP* keys) means that lost keys render those data stores unrecoverable even if there are backups.

2. Two hosts not connected to the Internet do not have backups outside of the ASL19 office. [[Redacted detail]].

Physical security: ASL19 office

The existence and location of the ASL19 office is expected to be not-public and difficult to locate. The address is not listed on any ASL19 website and no reference to it could be found online. Mailed communications are addressed to a P.O. Box, although some magazines and other materials are mailed directly to the office with addressing / labels that mention that the addressee is ASL19.

Access control

Access is restricted to the ASL19 office through a door that is locked at all times. An attempt to enter the building required self-identification through a voice intercom system and a manual opening of the main door by a staff member of ASL19.

[[Redacted detail]].

Redacted section

[[Redacted section at request of ASL19]].

Physical intrusion detection

The ASL19 office has an alarm system with central monitoring. Each ASL19 employee has their own individual code for activating / de-activating the alarm that is provisioned to them when they are onboarded. There is only one staff member who is able to create or remove access codes through an authentication process with the management company.

[[Redacted]].

A motion detector is present in the ASL19 office and was confirmed to be operational.

Guests

Guests are not common at the ASL19 office, and caution is exercised when invitations are made. Guests can be given Wi-Fi access on a special network, but this is not very common.

V-015: Redacted finding

[[Redacted section at request of ASL19]].

V-016: Redacted finding

[[Redacted section at request of ASL19]].