THE TOP 5 OVERLOOKED AREAS TO COVER IN YOUR NEXT SECURITY AUDIT

Cyolo

Becoming a cybersecurity statistic is no joke. According to a recent report, an external hacker can access the corporate network in 93% of organizations. It is, therefore, essential to prepare the best possible defense against all types of cyberattack.

As one part of standard cyber-preparedness, organizations must perform regular security audits. A security audit is a vital cog in a machine that provides the intelligence needed to apply and enforce the right levels of cybersecurity measures. But often, security audits fall short: key areas are forgotten, and holes appear in even the best-laid security plans.

Here are five critical areas to include in your next security audit to make sure you close all gaps.

SECURITY AUDIT AREA 1

Legacy Applications

THE AUDIT AREA

It is well known that legacy applications are still part of most organizations' Information Technology (IT) real estate. Gartner predicts that 90% of current applications will still hang around the network in 2025. Insufficient access control measures to legacy applications are one of the reasons why security audits fail. Legacy applications are notorious for lacking support for modern access control mechanisms and protocols, which leads to high levels of inappropriate access and a host of security issues.

THE FIX

Locate all your legacy applications to build up a legacy application profile. This can be done using software platforms that provide discovery services. It is also essential to extend your discovery exercise to third-party applications as well as homegrown applications. Once located, develop a plan to add multi-factor authentication (MFA) and single sign-on (SSO) capabilities to these systems. Part of the problem with legacy applications is that they do not natively support MFA and SSO. Fortunately, there are now identity-centric access control platforms that overlay MFA and SSO on legacy applications to fix previously unbridgeable gaps.

SECURITY AUDIT AREA 2

Integrating Multiple Identity Sources

THE AUDIT AREA

Like legacy applications, identity providers (IdPs) often become more of a sprawl than a focused solution in an enterprise. This is because an enterprise may add IdPs across the expanded network to provide identity provisioning for various employees, third-party users, and even devices. Also, during a merger or acquisition, external IdPs may need to be co-opted into the parent organization. IdP sprawl must be carefully managed to prevent security vulnerabilities from propagating. It also requires careful governance to avoid duplicate identities and to ensure least privilege principles are upheld.

THE FIX

Even if your organization has multiple IdPs, ensuring that these IdPs work together is crucial. Federating multiple IdPs is the answer to IdP sprawl. Using a platform such as Cyolo, IdPs are integrated with all your applications. This includes legacy applications, even if these are older applications that do not support the languages necessary to work with modern IdPs. The result is a seamless end-user experience and a more secure access control setup. In addition, multiple IdPs become homogenized, and users are seamlessly authenticated from a single interface.

SECURITY AUDIT AREA 3

User Access Permissions

THE AUDIT AREA

Another important area that security audits may miss out on is access privileges. This covers the who, what, and where of access controls: who is entitled to access what, when they are allowed that access, and where the access occurs. More than privileged account management, this area focusses on the role based application entitlement. According to Forrester, 80% of data breaches are caused by misusing privileged credentials. It is vital to determine if users have more access rights than needed to do their job, but this foundational cybersecurity principle is often challenging to enforce.

THE FIX

Before beginning your official security audit, perform a preliminary audit of the access rights of users inside and outside your organization. As part of this exercise, identify and assess privileged access rights. Then, use the principle of least privilege to optimize access permissions. Zero-trust access solutions provide a way to enforce least privilege access by continuously verifying access attempts. This verification is performed before and after access, ensuring that all identities are authenticated and both internal and external attacks are mitigated. The access privileges should also be revoked as soon as the user connection is terminated so that each user is authenticated every time they access the resource.

SECURITY AUDIT AREA 4

Incident Response and Mitigation

THE AUDIT AREA

The faster an organization can detect an incident, the greater chance they can contain the damage. Unfortunately, an IBM report found that it takes about 212 days to discover a breach and another 75 days to contain it. Add stolen credentials into the mix, and this becomes even more of a challenge. Data breaches associated with stolen or compromised credentials took 327 days, or nearly 11 months, to detect.

THE FIX

Identification, response, and mitigation are the keys to controlling and containing a security incident. Therefore, it is vital to have a robust incident response and mitigation plan to reduce the time to detect a compromise. Because privileged access credentials add complexity and time to incident detection, the ability to revoke privileged access in real-time is critical. Ensure that your zero-trust identity solution includes a mechanism to promptly shut down user access, including privileged user access, if anomalous behavior or a compromised account is identified.

SECURITY AUDIT AREA 5

Audit and Compliance

THE AUDIT AREA

Data protection and privacy regulations are costly in terms of both time and human resources. Non-compliance fines can also be breathtaking. Cumulative fines for GDPR non-compliance already add up to over $2 billion. The California equivalent of GDPR, the CCPA, also issues hefty penalties; a recent privacy violation case involving Zoom cost the company $85 million. An audit can ensure that your organization is compliant with data protection regulations. A subset of the security audit should focus on compliance and privacy. Data protection assessments regarding compliance needs can also provide the intelligence needed to support the forensic analysis of data security measures.

THE FIX

Overall security audits should include a compliance audit that focuses on specifics associated with the data type and privacy protection regulations impacting geography and/or the industry sector. These audits should focus on security measures, data availability, processing integrity, and the confidentiality and privacy controls used. An essential element of a compliance audit is classifying data; this provides a template to ensure the correct level of protection is applied. Full-lifecycle audit of data should include how the data is collected or generated and retention policies associated with these data. This lifecycle audit should also assess user access to an application and the level of user privileges associated with each class of data.

BONUS SECURITY AUDIT AREA

Vendor Zero-Trust Compliance

THE AUDIT AREA

The concept of zero-trust security has emerged to counterbalance the increasingly complex nature of modern cyberattacks. A zero-trust approach is already mandated for government agencies in the United States with a 2021 Executive Order stating, “The Federal Government must adopt security best practices; advance toward Zero Trust Architecture.” This acceptance of the zero-trust model and movement toward its implementation is no doubt a positive; however, there is too little emphasis placed on confirming whether zero-trust vendors are actually practicing what they preach and adhering to the principles of zero trust within their own infrastructure.

THE FIX

Security audits should check the use of zero-trust policies across vendor ecosystems. Determining whether you provide your suppliers with highly sensitive information, such as passwords and encryption keys, is crucial - but so is ensuring that your vendor actually abides by the principles of zero trust. Security vendors who decrypt customer data or store such data in their own clouds and ecosystems pose the risk of becoming a single point of failure for your entire zero-trust system.

LEAVE NO STONE UNTURNED

Conducting regular security audits is a vital part of ensuring that you are doing everything possible to prevent a cyberattack or accidental data leak. But vulnerabilities often creep in – and in unexpected areas.

The five (plus a bonus!) areas highlighted here should be included in your next security audit to leave no digital stone unturned.

Cyolo

cyolo.io