Kỹ sư bảo mật

I, Kỹ sư bảo mật là gì

Tại sao các tổ chức cần bảo mật?

Trong thời đại internet, việc biến đổi cách thức hoạt động của tổ chức trên toàn cầu cũng mang đến những thách thức. Mặc dù không thể phủ nhận rằng công nghệ đã làm cuộc sống của tổ chức dễ dàng hơn rất nhiều bằng cách mở ra những cánh cửa mới để hợp tác và đổi mới, chúng ta thường nghe nói về các tổ chức bị tấn công, mất dữ liệu khách hàng, bị tống tiền và đối mặt với các loại tấn công mạng khác. Để đối phó với những mối đe dọa này, tổ chức có thể quay trở lại cách thức kinh doanh cũ mà không nhận được sự hỗ trợ từ công nghệ hiện đại, đặt họ vào thế bất lợi, hoặc họ có thể tiến lên phía trước và đảm bảo an ninh phần kỹ thuật số của doanh nghiệp. Do đó, giống như bất kỳ tổ chức nào sẽ bảo vệ tài sản vật lý và dành toàn bộ các phòng ban cho việc này, tài sản kỹ thuật số của một công ty cũng phải được bảo vệ. Cần lưu ý rằng tổ chức làm tất cả điều này để đảm bảo mục tiêu chính của họ được đạt được mà không bị cản trở.

Vai trò của một kỹ sư bảo mật

Đáp ứng nhu cầu bảo mật được đề cập trên, các tổ chức thuê kỹ sư bảo mật. Để thuê một kỹ sư bảo mật, một tổ chức coi một kỹ sư bảo mật là người:

- Phụ trách bảo mật tổng thể của tổ chức. Người chịu trách nhiệm chính cho việc bảo vệ tài sản kỹ thuật số của tổ chức.

- Đảm bảo rằng rủi ro an ninh mạng của tổ chức được giảm thiểu trong suốt thời gian.
- Tạo ra chiến lược và xây dựng các hệ thống giảm thiểu rủi ro do các mối đe dọa an ninh mạng gây ra cho tổ chức.
- Định kỳ tiến hành các kiểm tra để đảm bảo tính mạnh mẽ của tư thế an ninh mạng của tổ chức, xác định điểm yếu và chuẩn bị các biện pháp giảm thiểu.
- Phát triển và triển khai các giải pháp mạng an toàn.
- Thiết kế và xây dựng các hệ thống đáng tin cậy, đáng tin cậy và an toàn.
- Hợp tác và phối hợp với các nhóm khác để thiết lập giao thức bảo mật trên toàn tổ chức.

Yêu cầu chuyên môn cho một kỹ sư bảo mật

Như bạn có thể nhận thấy, vai trò kỹ sư bảo mật đã được đề cập ở trên rất rộng và có thể yêu cầu một phòng ban hoàn chỉnh thay vì chỉ một người. Điều này bởi vì vai trò này được định nghĩa một cách mơ hồ và khác nhautùy từng tổ chức. Một kỹ sư bảo mật tiếp cận các vấn đề lớn, chia nhỏ chúng thành các phần nhỏ hơn, và sau đó giải quyết chúng. Do đó, một kỹ sư bảo mật là người tuân thủ quy trình này để giải quyết các vấn đề bảo mật. Điều này có nghĩa là mặc dù bạn có một mô tả công việc, mỗi ngày có thể khá khác nhau vì bạn đối mặt với các vấn đề khác nhau. Nhìn chung, khi thuê một kỹ sư bảo mật, tổ chức tìm kiếm các yêu cầu cơ bản sau:

- 0-2 năm kinh nghiệm với quản trị IT, trợ giúp mạng hoặc hoạt động bảo mật.
- Hiểu biết cơ bản về mạng máy tính, hệ điều hành và lập trình.
- Hiểu biết căn bản về các khái niệm bảo mật như Quản trị, Rủi ro và Tuân thủ (GRC).

Answer the questions below

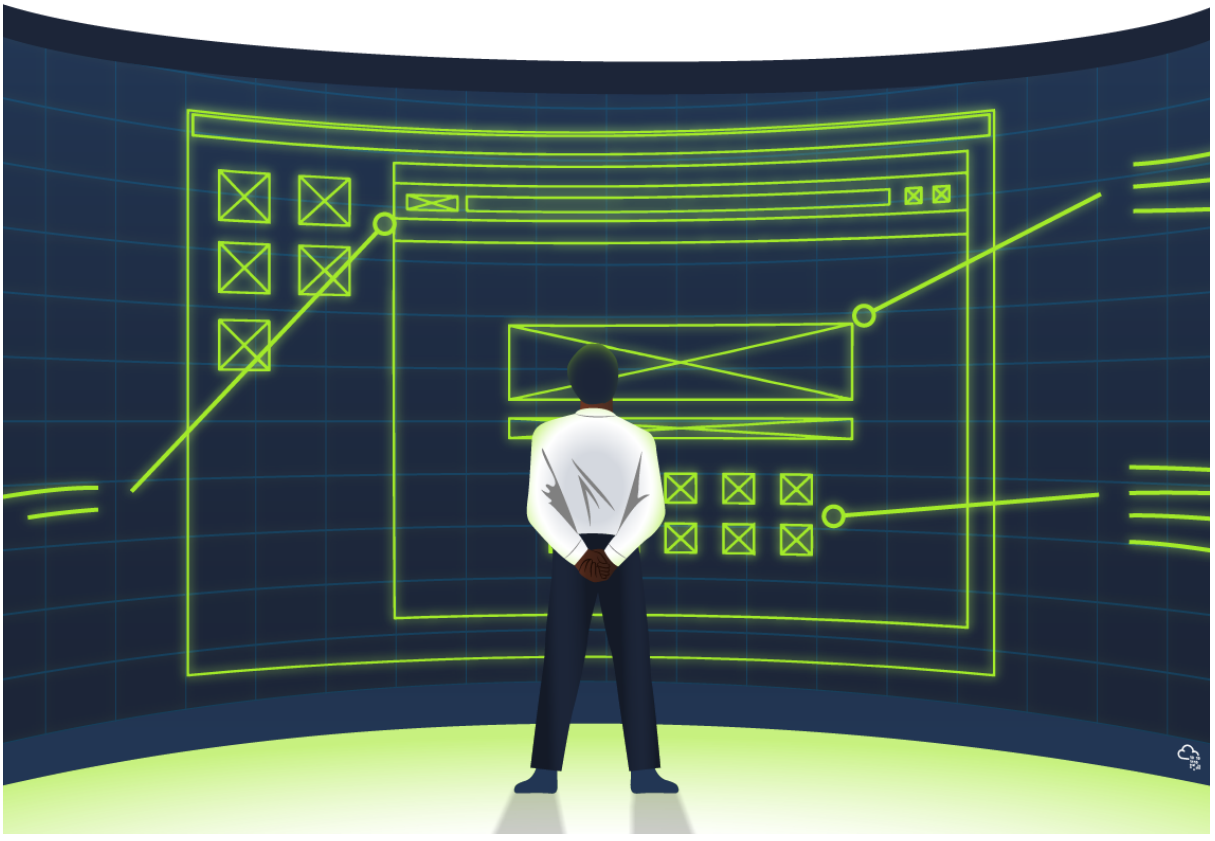
Who ensures that an organization's cyber security risk is minimized at all times?

Security Engineer

II, Trách nhiệm cốt lõi của một kỹ sư bảo mật

Quản lý tài sản/Kiểm kê tài sản

Một trong những bước chính để đảm bảo an ninh của một tổ chức là duy trì phiếu kiểm kê tài sản của tổ chức. Trong thuật ngữ an ninh mạng, điều này có nghĩa là quản lý và duy trì một danh sách tài sản kỹ thuật số của tổ chức. Kỹ sư bảo mật chỉ có thể chịu trách nhiệm bảo mật của tổ chức nếu họ biết tổ chức có những tài sản nào. Họ cũng phải đảm bảo rằng danh sách tài sản này được duy trì và cập nhật đều đặn và bao gồm đầy đủ thông tin về tài sản như tên tài sản, loại tài sản, địa chỉ IP, vị trí vật lý, vị trí trong mạng, ứng dụng đang chạy trên tài sản, quyền truy cập (chỉ trong tổ chức hoặc công khai), và chi tiết chủ sở hữu tài sản.



Chính sách bảo mật

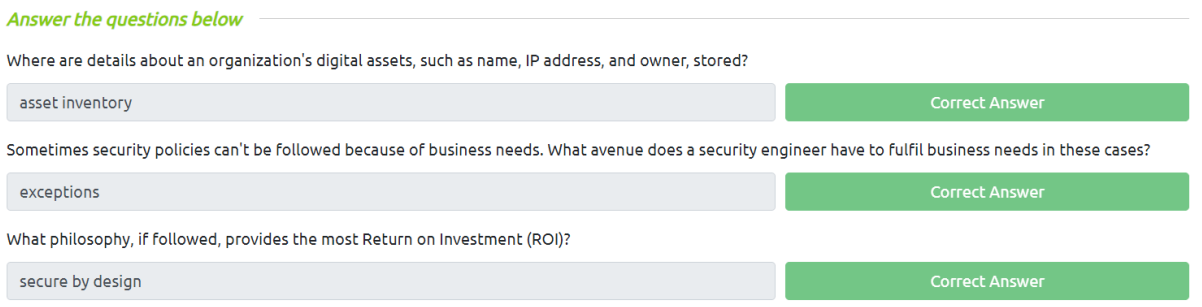
Một tổ chức cần có chính sách bảo mật mạnh để duy trì tư thế bảo mật vững chắc. Một kỹ sư bảo mật giúp tổ chức tạo ra chính sách bảo mật dựa trên các Nguyên tắc Bảo mật đã được thiết lập. Những chính sách này sau đó được triển khai trên toàn tổ chức, và kỹ sư bảo mật đảm bảo rằng việc triển khai tuân thủ đúng ý và tinh thần của các chính sách. Đôi khi, có nhu cầu cấp phép cho các ngoại lệ đối với chính sách bảo mật do nhu cầu kinh doanh. Trong tình huống như vậy, kỹ sư bảo mật tham khảo các nguyên tắc bảo mật để cho phép hoặc từ chối các ngoại lệ và đề xuất biện pháp giảm thiểu rủi ro.

An toàn bằng thiết kế

Một kỹ sư bảo mật đảm bảo rằng tổ chức được an toàn bằng thiết kế. Kỹ sư hiểu rằng tư thế bảo mật đạt được lợi nhuận cao nhất nếu tuân thủ triết lý an toàn bằng thiết kế. Điều này có nghĩa là kỹ sư bảo mật thực hiện các bước để triển khai Kiến trúc Mạng An toàn, đảm bảo rằng hệ điều hành Windows, Linux và Active Directory của tổ chức được tăng cường bảo mật, và phát triển phần mềm tuân thủ Chu kỳ Phát triển Phần mềm An toàn.

Đánh giá và đảm bảo an ninh

Mặc dù thiết kế an toàn cho mạng và cơ sở hạ tầng của tổ chức có thể là một bước đầu tuyệt vời, kỹ sư bảo mật hiểu rằng công việc của họ không chỉ kết thúc ở đó. Họ hiểu rằng an ninh là công việc khó khăn yêu cầu nỗ lực liên tục. Trong khi kỹ sư bảo mật phải đảm bảo mọi thứ được thực hiện đúng, họ cũng hiểu rằng chỉ cần một lỗ hổng duy nhất thì một cuộc tấn công có thể thành công. Để giảm thiểu rủi ro từ cảnh quan đe dọa liên tục tiến triển, một kỹ sư bảo mật lên kế hoạch tiến hành đánh giá bảo mật, kiểm tra và các bài tập đội màu đỏ và đội màu tím thường xuyên để liên tục cải thiện tư thế bảo mật. Mặc dù kỹ sư bảo mật có thể không thực hiện các đánh giá và kiểm tra mình, họ tham gia chủ yếu trong việc giúp lập lịch cho các hoạt động này, tạo ra Yêu cầu Báo giá (RFQs) cho các bên ngoài thực hiện các hoạt động này, và giúp ưu tiên và thực hiện các phát hiện từ các hoạt động này.



III, Cải tiến không ngừng

Một kế hoạch bảo mật vững chắc cho tổ chức không chỉ là một công việc một lần mà là một nỗ lực liên tục. Tương tự, công việc của kỹ sư bảo mật không kết thúc sau khi các chính sách được thiết kế và triển khai. Thực tế, đó là một cuộc hành trình để liên tục cải tiến. Các bước sau đây giúp kỹ sư bảo mật thực hiện vai trò này.

Đảm bảo nhận thức:
Một kỹ sư bảo mật có thể được giao nhiệm vụ duy trì một mức độ nhận thức bảo mật nhất định trong tổ chức. Con người là nền tảng của bất kỳ tổ chức nào, và như

thường được nói, con người là điểm yếu của bảo mật tổ chức. Kỹ sư bảo mật định kỳ tổ chức các buổi nhận thức nhằm mục tiêu chính là tấn công xã hội để đảm bảo rằng con người không mắc sai lầm có thể đe dọa bảo mật của tổ chức. Các buổi nhận thức cũng được tổ chức cho các nhóm cụ thể để đảm bảo rằng họ tuân theo các nguyên tắc bảo mật liên quan đến lĩnh vực chuyên môn của họ, chẳng hạn như phát triển phần mềm an toàn hoặc kiến trúc mạng an toàn.

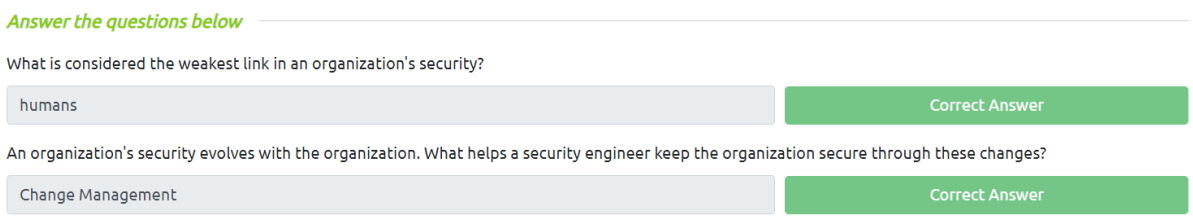
Quản lý rủi ro:
Ban lãnh đạo điều hành của hầu hết các tổ chức nhìn nhận bảo mật từ góc nhìn giảm thiểu rủi ro. Bảo mật là rất quan trọng đối với doanh nghiệp vì bỏ qua nó có thể dẫn đến gián đoạn hoạt động, rò rỉ dữ liệu, vụ kiện hoặc các hình thức rủi ro khác. Do đó, thường kỹ sư bảo mật được giao nhiệm vụ xác định các rủi ro bảo mật, xác định khả năng xảy ra và tác động của chúng, và tìm giải pháp để giảm thiểu những rủi ro đó. Cần lưu ý rằng không phải lúc nào cũng có thể loại bỏ hoàn toàn tất cả các rủi ro khi vận hành hoạt động kinh doanh. Đôi khi, phải đưa ra quyết định chấp nhận một rủi ro và tiếp tục. Trong tình huống như vậy, kỹ sư bảo mật có thể thực hiện một số biện pháp hạn chế để giảm thiểu rủi ro. Việc chấp nhận hoặc hạn chế rủi ro thường là một quyết định kinh doanh, và kỹ sư bảo mật đóng vai trò là một cố vấn đáng tin cậy của ban lãnh đạo giúp họ đưa ra quyết định này bằng cách cung cấp chuyên môn về chủ đề. Hãy lấy ví dụ về một tổ chức sử dụng phần mềm cơ sở dữ liệu cho chuỗi cung ứng của mình chạy trên phiên bản Linux có lỗ hổng. Phần mềmCảm ơn bạn đã cung cấp thêm thông tin về vai trò của một kỹ sư bảo mật trong việc duy trì một tư thế bảo mật đáng tin cậy. Điều quan trọng là các tổ chức có những chuyên gia riêng biệt luôn theo dõi và cải tiến các biện pháp bảo mật để bảo vệ khỏi các mối đe dọa tiến triển. Các bước mà bạn đã đề cập, như đảm bảo nhận thức, quản lý rủi ro, quản lý thay đổi, quản lý lỗ hổng và tuân thủ và kiểm toán, thực sự là quan trọng để duy trì một tư thế bảo mật mạnh mẽ. Bằng cách tuân thủ các bước này, kỹ sư bảo mật có thể giúp các tổ chức tự động phát hiện và giải quyết các lỗ hổng tiềm tàng hoặc các vấn đề không tuân thủ quy định.

Quản lý thay đổi
Các tổ chức tiếp tục tiến triển theo thời gian, đồng thời cũng dẫn đến sự thay đổi trong tư thế bảo mật của chúng. Để đảm bảo một tư thế bảo mật mạnh mẽ, kỹ sư bảo mật theo dõi các thay đổi trong tài sản kỹ thuật số của tổ chức có thể ảnh hưởng đến tư thế bảo mật và đưa ra biện pháp để cải thiện tư thế bảo mật theo sự phát triển của tổ chức. Hãy giả sử một tổ chức muốn nâng cấp mô-đun thương mại điện tử trên trang web của mình dành cho khách hàng doanh nghiệp. Mô-đun mới sẽ yêu cầu một đánh giá rủi ro, kiểm tra xâm nhập và đánh giá lỗ hổng trước khi tích hợp vào trang web. Kỹ sư bảo mật sẽ đảm bảo rằng tất cả những yêu cầu này được đáp ứng và tích hợp mới sẽ không tạo ra lỗ hổng bảo mật. Hơn nữa, cũng sẽ đảm

bảo rằng mô-đun mới tuân theo tất cả các chính sách và hướng dẫn về bảo mật do tổ chức đề ra.

Quản lý lỗ hổng
Cảnh với mối đe dọa liên tục. Các phiên bản phần mềm mới được phát hành và lỗ hổng được phát hiện trong các phiên bản cũ hơn. Công việc của kỹ sư bảo mật thường bao gồm theo dõi các lỗ hổng trong toàn bộ tổ chức và lập kế hoạch vá hoặc giảm thiểu rủi ro của chúng. Các lỗ hổng thường được vá theo mức độ nghiêm trọng, như chúng ta sẽ tìm hiểu trong phòng Quản lý lỗ hổng.

Tuân thủ và Kiểm toán
Một phần quan trọng của công việc của kỹ sư bảo mật là đảm bảo tuân thủ các yêu cầu về quy định và tổ chức. Tùy thuộc vào ngành công nghiệp, khách hàng và vị trí của tổ chức, nó có thể phải tuân theo các tiêu chuẩn tuân thủ khác nhau như PCI-DSS, HIPAA, SOC2, ISO27001, NIST-800-53 và nhiều hơn nữa. Kỹ sư bảo mật làm việc chặt chẽ với các kiểm toán viên nội bộ và bên ngoài để phát hiện bất kỳ vấn đề không tuân thủ nào và giải quyết chúng một cách hiệu quả. Ngoài ra, họ có trách nhiệm duy trì các chứng chỉ bảo mật của tổ chức theo yêu cầu.



IV, Các Vai trò và Trách nhiệm Bổ sung

Quản lý Công cụ Bảo mật

Đôi khi, kỹ sư bảo mật có thể được yêu cầu cấu hình hoặc điều chỉnh các công cụ bảo mật như SIEM, Firewall, WAF, EDR và nhiều hơn nữa. Trong một số tổ chức, đó cũng có thể là trách nhiệm chính của một kỹ sư bảo mật. Trong vai trò như vậy, kỹ sư bảo mật có thể đưa ra quyết định hoặc cung cấp thông tin cho người ra quyết định về việc mua công cụ dựa trên yêu cầu của tổ chức và đánh giá của kỹ sư về các công cụ cạnh tranh.

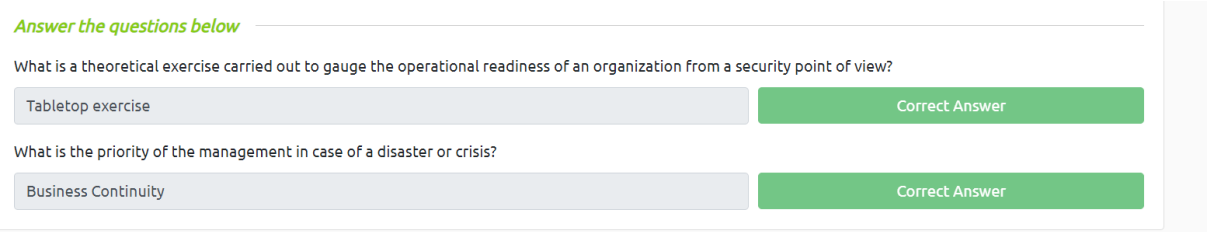
Bài tập Mô phỏng

Bài tập mô phỏng thường được tiến hành để đánh giá sự sẵn sàng vận hành của một tổ chức từ góc nhìn bảo mật. Các kịch bản cụ thể được xác định để được thực

hiện và các thành viên trong nhóm bảo mật phải giải thích vai trò của họ trong các kịch bản đang được thảo luận. Ví dụ, một kịch bản có thể bao gồm việc xâm nhập vào một thiết bị cuối thông qua một email lừa đảo. Tất cả các thành viên trong nhóm sẽ giải thích các bước tương ứng theo hướng dẫn của tổ chức. Đôi khi, kỹ sư bảo mật được yêu cầu tiến hành những bài tập mô phỏng này.

Phục hồi sau thảm họa và Quản lý khủng hoảng

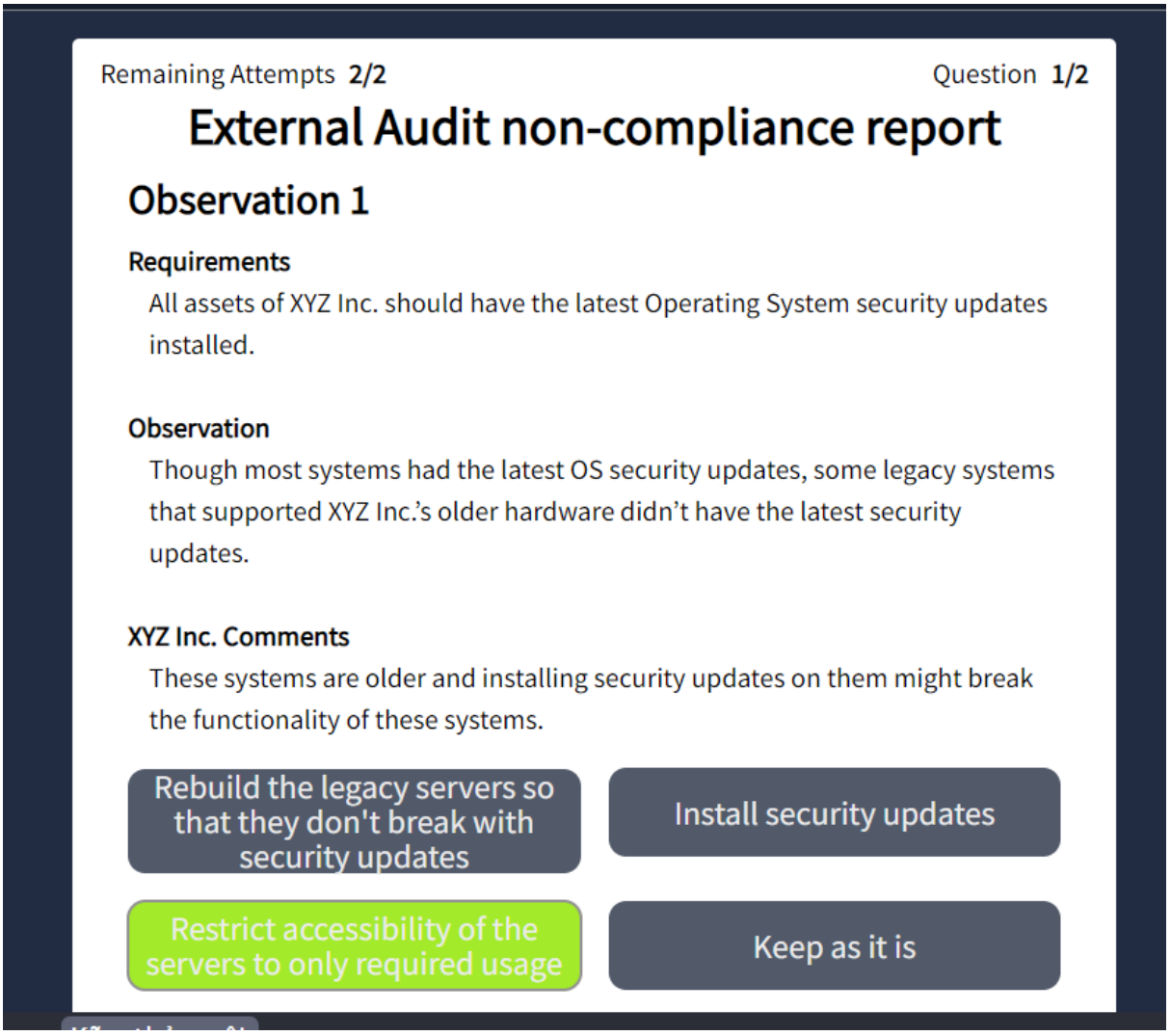
Một tư thế bảo mật mạnh mẽ yêu cầu tổ chức lập kế hoạch cho các sự cố bất ngờ, thảm họa hoặc khủng hoảng. Trong bất kỳ kịch bản nào như vậy, ưu tiên hàng đầu của ban quản lý là duy trì tính liên tục của hoạt động kinh doanh. Kỹ sư bảo mật có thể tham gia vào việc lập kế hoạch phục hồi sau thảm họa, duy trì tính liên tục kinh doanh và quản lý khủng hoảng như một phần của các khung hợp tuân thủ khác nhau và các chính sách nội bộ của tổ chức. Vai trò của kỹ sư bảo mật trong các lĩnh vực này có thể khác nhau tùy thuộc vào tổ chức.



V, Walking in Their Shoes

Trong quá trình thực hiện nhiệm vụ của mình, các kỹ sư bảo mật phải xem xét các khía cạnh khác nhau của việc điều hành một doanh nghiệp ngoài việc giữ cho nó an toàn. Những yếu tố này có thể bao gồm hoạt động kinh doanh, chi phí, sự dễ triển khai, sự dễ sử dụng và nhiều hơn nữa. Mặc dù hệ thống an toàn nhất là hệ thống bị tắt và ngừng kết nối với nguồn điện, nhưng hệ thống như vậy sẽ không đạt được bất kỳ mục tiêu kinh doanh nào. Do đó, một kỹ sư bảo mật phải xem xét mục tiêu kinh doanh và an ninh khi đưa ra quyết định.

Question


Remaining Attempts 2/2
Question 1/2
External Audit non-compliance report
Observation 1
Requirements
All assets of XYZ Inc. should have the latest Operating System security updates installed.
Observation
Though most systems had the latest OS security updates, some legacy systems that supported XYZ Inc.'s older hardware didn't have the latest security updates.
XYZ Inc. Comments
These systems are older and installing security updates on them might break the functionality of these systems.
Rebuild the legacy servers so that they don't break with security updates
Install security updates
Restrict accessibility of the servers to only required usage
Keep as it is

Remaining Attempts **2/2** Question **2/2**

External Audit non-compliance report

Observation 2

Requirements

All network communication, user activity,and security device logs shall be aggregated in a single platform (SIEM) and monitored continuously.

Observation

XYZ Inc. has some assets in the cloud and others on-prem. It was observed that the cloud assets were not integrated with the SIEM, which is present on-prem.

XYZ Inc. Comments

The logs from the cloud are not integrated with the SIEM because this will require enabling internet access to the SIEM, which is not desirable.

Forward cloud logs to SIEM regardless of concerns of XYZ Inc

Keep as it is

Aggregate cloud logs in a single place. Forward the logs from that place to on-prem network using a restricted tunnel

Rebuild the applications on the cloud to on-prem or vice versa

Vulnerability 1

Asset Name

Oracle-backend-DB-Server

ORACLE MYSQL VULNERABILITY: CVE-2022-21417

Description

Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 5.7.37 and prior and 8.0.28 and prior. Easily exploitable vulnerability allows a high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).

Recommended Solution

Upgrade to the latest version of Oracle MySQL

Download and apply the upgrade from:

http://dev.mysql.com/downloads/mysql

Keep as it is

Rebuild the server

Restrict accessibility of the server only through VPN or internal network

Patch the vulnerability

Remaining Attempts **2/2** Question **2/3**

VAPT report

Vulnerability 2

Asset Name

corporate-client-portal

OPENSSL THE C_REHASH SCRIPT ALLOWS COMMAND INJECTION (CVE-2022-2068)

Description

In addition to the c_rehash shell command injection identified in CVE-2022-1292, further circumstances where the c_rehash script does not properly sanitise shell metacharacters to prevent command injection were found by code review. When the CVE-2022-1292 was fixed, it was not discovered that there were other places in the script where the file names of certificates being hashed were possibly passed to a command executed through the shell. This script is distributed by some operating systems in a manner where it is automatically executed. On such operating systems, an attacker could execute arbitrary commands with the privileges of the script. Use of the c_rehash script is considered obsolete and should be replaced by the OpenSSL rehash command line tool. Fixed in OpenSSL 3.0.4 (Affected 3.0.0,3.0.1,3.0.2,3.0.3). Fixed in OpenSSL 1.1.1p (Affected 1.1.1-1.1.1o). Fixed in OpenSSL 1.0.2zf (Affected 1.0.2-1.0.2ze).

Recommended Solution

- Upgrade to OpenSSL version 1.0.2zf
- Download and apply the upgrade from: http://ftp.openssl.org/source/openssl1.0.2zf.tar.gz

  > Upgrade to version 1.0.2zf of OpenSSL (http://www.openssl.org). The source code for this release can be downloaded from OpenSSL's website(http://ftp.openssl.org/source/openssl-1.0.2zf.tar.gz). To obtain binaries for your platform, please visit your vendor's site. Please note that many operating system vendors choose to apply the most recent OpenSSL security patches to their distributions without changing the package version to the most recent OpenSSL version number.

- Upgrade to OpenSSL version 1.1.1p
- Download and apply the upgrade from: http://ftp.openssl.org/source/openssl1.1.1p.tar.gz Upgrade to version 1.1.1p of OpenSSL (http://www.openssl.org). The source code for this release can be downloaded from OpenSSL's website (http://ftp.openssl.org/source/openssl-1.1.1p.tar.gz). To obtain binaries for your platform, please visit your vendor's site. Please note that many operating system vendors choose to apply the most recent OpenSSL security patches to their distributions without changing the package version to the most recent OpenSSL version number.

- Upgrade to OpenSSL version 3.0.4 Download and apply the upgrade from: http://ftp.openssl.org/source/openssl-3.0.4.tar.gz Upgrade to version 3.0.4 of OpenSSL (http://www.openssl.org). The source code for this release can be downloaded from OpenSSL's website (http://ftp.openssl.org/source/openssl-3.0.4.tar.gz). To obtain binaries for your platform, please visit your vendor's site. Please note that many operating system vendors choose to apply the most recent OpenSSL security patches to their distributions without changing the package version to the most recent OpenSSL version number.

Vulnerability 3

Asset Name

corporate-website-public

APACHE HTTPD: MOD_LUA USE OF UNINITIALIZED VALUE OF IN R:PARSEBODY (CVE-2022-22719)

Description

A carefully crafted request body can cause a read to a random memory area which could cause the process to crash. This issue affects Apache HTTP Server 2.4.52 and earlier.

Recommended Solution

- Apache HTTPD >= 2.4 and < 2.4.53
- Upgrade to Apache HTTPD version 2.4.53
- Apache HTTPD version 2.4.53 Download and apply the upgrade from: http://archive.apache.org/dist/httpd/httpd2.4.53.tar.gz
- Many platforms and distributions provide pre-built binary packages for Apache HTTP server. These pre-built packages are usually customized and optimized for a particular distribution, therefore we recommend that you use the packages if they are available for your operating system.

Restrict accessibility of the server only through VPN or internal network

Keep as it is

Rebuild the server

Patch the vulnerability

Flag

THM{S3CUR1TY_3NG1N33R5_R0CK}