## Security Audit

**W ramach kursu Google Cybersecurity Professional Certificate wykonujemy zadanie polegające na przeprowadzeniu wewnętrznego audytu bezpieczeństwa w fikcyjnej organizacji.**

**Scenariusz:**

*Ten scenariusz jest oparty na fikcyjnej firmie:*

Botium Toys to mała amerykańska firma zajmująca się rozwojem i sprzedażą zabawek. Firma ma jedną fizyczną lokalizację. Jednak jego obecność w Internecie wzrosła, przyciągając klientów w Stanach Zjednoczonych i za granicą. Ich dział technologii informatycznych (IT) znajduje się pod rosnącą presją, aby wspierać ich rynek internetowy na całym świecie.

Kierownik działu IT zdecydował o konieczności przeprowadzenia wewnętrznego audytu informatycznego. Wyraża obawy związane z brakiem utrwalonego planu działania w celu zapewnienia ciągłości biznesowej i zgodności w miarę rozwoju firmy. Wierzy, że audyt wewnętrzny może pomóc lepiej zabezpieczyć infrastrukturę firmy oraz pomóc zidentyfikować i ograniczyć potencjalne ryzyko, zagrożenia lub słabe punkty krytycznych aktywów. Zarządzający jest również zainteresowany przestrzeganiem przez nich przepisów związanych z przyjmowaniem płatności internetowych i prowadzeniem działalności gospodarczej na terenie Unii Europejskiej (UE).

Menedżer IT zaczyna od wdrożenia ram bezpieczeństwa cybernetycznego Narodowego Instytutu Standardów i Technologii (NIST CSF), ustalenia zakresu i celów audytu oraz przeprowadzenia oceny ryzyka. Celem audytu jest przedstawienie przeglądu zagrożeń, jakie firma może napotkać w związku z obecnym stanem bezpieczeństwa. Kierownik IT chce wykorzystać wyniki audytu jako dowód w celu uzyskania zgody na rozbudowę swojego działu.

**Krok 1: Analiza zakresu audytu, celów i oceny ryzyka.**

Otrzymaliśmy od naszego menadżera IT raporty na temat celów i zasięgów audytu oraz ocenę ryzyka. W skrócie wygląda to tak:

**Cele:**

* Poprawić obecny poziom bezpieczeństwa Botium Toys, dostosowując się do najlepszych praktyk branżowych (np. przestrzegać NIST CSF, wdrażać koncepcję najmniejszych uprawnień)
* Zapewnić zalecenia dotyczące łagodzenia skutków (tj. kontrole, zasady, dokumentację) w oparciu o bieżące ryzyka
* Identyfikacja przepisów dotyczące zgodności, których Botium Toys musi przestrzegać, przede wszystkim w oparciu o to, gdzie prowadzimy działalność i jak przyjmujemy płatności]
* Dokładny raport znajdziemy w dokumencie **Botium Toys: Audit Scope and goals** znajdziemy go w folderze audytu

**Ryzyka:**

* Nieodpowiednie zarządzanie aktywami
* Nie ma odpowiednich kontroli
* Może nie być zgodny z amerykańskimi i międzynarodowymi przepisami i wytycznymi
* Obecna ocena ryzyka to 8/10 (wysoka), ze względu na brak kontroli i przestrzegania przepisów i standardów zgodności
* Dokładny raport znajdziemy w dokumencie **Botium Toys: Risk assessment** znajdziemy go w folderze audytu

Po zaznajomieniu się z dokumentami powinniśmy zastanowić się nad następującymi pytaniami:

* Jakie są największe zagrożenia dla organizacji?
* Które kontrole są najważniejsze do natychmiastowego wdrożenia, a które w przyszłości?
* Jakich przepisów dotyczących zgodności musi przestrzegać firma Botium Toys, aby zapewnić bezpieczeństwo danych klientów i dostawców, uniknąć kar itp.?

**Krok 2: Przeprowadź audyt: ocena kontroli**

# Control checklist

| **Administrative Controls** | | | |
| --- | --- | --- | --- |
| **Control Name** | **Control type and explanation** | **Needs to be implemented (X)** | **Priority** |
| Least Privilege | Preventative; reduces risk by making sure vendors and non-authorized staff only have access to the assets/data they need to do their jobs | X | High |
| Disaster recovery plans | Corrective; business continuity to ensure systems are able to run in the event of an incident/there is limited to no loss of productivity downtime/impact to system components, including: computer room environment (air conditioning, power supply, etc.); hardware (servers, employee equipment); connectivity (internal network, wireless); applications (email, electronic data); data and restoration | X | High |
| Password policies | Preventative; establish password strength rules to improve security/reduce likelihood of account compromise through brute force or dictionary attack techniques | X | High |
| Access control policies | Preventative; increase confidentiality and integrity of data | X | High |
| Account management policies | Preventative; reduce attack surface and limit overall impact from disgruntled/former employees | X | Medium |
| Separation of duties | Preventative; ensure no one has so much access that they can abuse the system for personal gain | X | High |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Technical Controls** | | | | | | |
| **Control Name** | | **Control type and explanation** | **Needs to be implemented**  **(X)** | | **Priority** | |
| Firewall | | Preventative; firewalls are already in place to filter unwanted/malicious traffic from entering internal network | *Already implemented* | | NA | |
| Intrusion Detection System (IDS) | | Detective; allows IT team to identify possible intrusions (e.g., anomalous traffic) quickly | *Already implemented* | | NA | |
| Encryption | | Deterrent; makes confidential information/data more secure (e.g., website payment transactions) | X | | High | |
| Backups | | Corrective; supports ongoing productivity in the case of an event; aligns to the disaster recovery plan | X | | High | |
| Password management system | | Corrective; password recovery, reset, lock out notifications | X | | High | |
| Antivirus (AV) software | | Corrective; detect and quarantine known threats | X | | High | |
| Manual monitoring, maintenance, and intervention | | Preventative/corrective; required for legacy systems to identify and mitigate potential threats, risks, and vulnerabilities | x | | High | |
| **Physical Controls** | | | | | | |
| **Control Name** | | **Control type and explanation** | | | **Needs to be implemented**  **(X)** | **Priority** |
| Time-controlled safe | | Deterrent; reduce attack surface/impact of physical threats | | | x | low |
| Adequate lighting | | Deterrent; limit “hiding” places to deter threats | | | x | low |
| Closed-circuit television (CCTV) surveillance | | Preventative/detective; can reduce risk of certain events; can be used after event for investigation | | | x | High |
| Locking cabinets (for network gear) | | Preventative; increase integrity by preventing unauthorized personnel/individuals from physically accessing/modifying network infrastructure gear | | | x | Medium |
| Signage indicating alarm service provider | | Deterrent; makes the likelihood of a successful attack seem low | | | x | low |
| Locks | | Preventative; physical and digital assets are more secure | | | x | High |
| Fire detection and prevention (fire alarm, sprinkler system, etc.) | | Detective/Preventative; detect fire in the toy store’s physical location to prevent damage to inventory, servers, etc. | | | x | Medium |

**Krok 3: Przeprowadź audyt: checklista zgodności**

# Compliance checklist

**\_\_\_\_\_ The Federal Energy Regulatory Commission - North American Electric**

**Reliability Corporation (FERC-NERC)**

The FERC-NERC regulation applies to organizations that work with electricity or that are involved with the U.S. and North American power grid. Organizations have an obligation to prepare for, mitigate, and report any potential security incident that can negatively affect the power grid. Organizations are legally required to adhere to the Critical Infrastructure Protection Reliability Standards (CIP) defined by the FERC.

**Explanation:**

**\_\_X\_\_ General Data Protection Regulation (GDPR)**

GDPR is a European Union (E.U.) general data regulation that protects the processing of E.U. citizens’ data and their right to privacy in and out of E.U. territory. Additionally, if a breach occurs and a E.U. citizen’s data is compromised, they must be informed within 72 hours of the incident.

**Explanation:** Firma Botium toys prowadzi interesy z klientami pochodzącymi z terytoriów Unii Europejskiej, tym samym regulacje dotyczące przetwarzania ich danych obejmują funkcjonowanie Botium toys.

**\_\_X\_\_ Payment Card Industry Data Security Standard (PCI DSS)**

PCI DSS is an international security standard meant to ensure that organizations storing, accepting, processing, and transmitting credit card information do so in a secure environment.

**Explanation:** Firma Botium Toys akceptuje transakcje za pomocą kard kredytowych, tym samym musi podlegać standardom PCI DSS.

**\_\_\_\_\_ The Health Insurance Portability and Accountability Act (HIPAA)**

HIPAA is a federal law established in 1996 to protect U.S. patients' health information. This law prohibits patient information from being shared without their consent. Organizations have a legal obligation to inform patients of a breach.

**Explanation:**

**\_\_X\_\_ System and Organizations Controls (SOC type 1, SOC type 2)**

The SOC1 and SOC2 are a series of reports that focus on an organization's user access policies at different organizational levels. They are used to assess an organization’s financial compliance and levels of risk. They also cover confidentiality, privacy, integrity, availability, security, and overall data safety. Control failures in these areas can lead to fraud.

**Explanation:** Firma Botium Toys operuje I przechowuje dane klientów tym samym musi zastosować się do regulacji **System and Organizations Controls**.

**Krok 4: Przeprowadź audyt: komunikacja z intersariuszami**

DO: IT Manager, Stakeholders

OD: Rami Matouk  
DATA: 06.07.2023  
TEMAT: Internal IT Audit Findings and Recommendations

Drodzy współpracownicy,

Prosimy o zapoznanie się z poniższymi informacjami dotyczącymi zakresu audytu wewnętrznego Botium Toys, celów, krytycznych ustaleń, podsumowania i zaleceń

**Zakres:**

* **Systemy: rozliczanie, wykrywanie punktów końcowych, zapory ogniowe, system wykrywania włamań, narzędzie SIEM.**
* **Kontrole: rozliczanie, wykrywanie punktów końcowych, zapory ogniowe, system wykrywania włamań, narzędzie SIEM.**
* **Procedury i protokoły określone dla systemów powyżej.**
* **Uprawnienia użytkownika**
* **Dostęp do sprzętu i systemu**

**Cele:**

* Przestrzegać standardów dotyczących NIST CSF
* Ustanowienie lepszych procesów dla naszych systemów
* Wzmocnienie kontroli systemów
* Implementacja konceptu najmniejszych przywileji
* Ustanowienie polityk i procedur wraz z ich poradnikami
* Upewnienie się w przestrzeganiu regulacji

**Krytyczne odkrycia** (muszą być zadresowane natychmiastowo):

* Organizacja musi natychmiast zaimplementować wiele systemów kontroli, aby spełnić cele audytu:

○ Kontrola najniższych uprawnień i podział obowiązków

○ Plany odzyskiwania po awarii

○ Zasady dotyczące haseł, kontroli dostępu i zarządzania kontami, w tym

wdrożenie systemu zarządzania hasłami

○ Szyfrowanie (dla bezpiecznych transakcji w witrynie)

○ Kopie zapasowe

○ Oprogramowanie AntiVirus

○ CCTV

○ Zamki

○ Ręczne monitorowanie, konserwacja i interwencja w starszych systemach

○ Systemy wykrywania i zapobiegania pożarom

* Należy przygotować polityki które spełniają wymogi PCI DSS oraz GDPR
* Powinno rozwinąć się procedury zgodne z SOC1 i SOC2

**Odkrycia** (powinny być zaadresowane kiedy znajdzie się okazja):

Kiedy będzie to możliwe należy zaimplementować:

○ Sejf sterowany czasowo

○ Odpowiednie oświetlenie

○ Zamykane szafki

○ Oznakowanie wskazujące dostawcę usług alarmowych

**Podsumowanie/Rekomendacje:**

Podsumowując rekomendujemy, aby braki w krytycznych systemach, kontrolach i politykach wprowadzić natychmiastowo. Ponieważ Botium Toys akceptuje płatności online od klientów z całego świata, należy implementować zmiany w pełnej zgodności z zaleceniami PCI DSS oraz GDPR. Ponieważ celem audytu jest wprowadzenie konceptu najmniejszych przywilejów powinny one powstać zgodnie z SOC1 oraz SOC2. Systemy backup i plany odzyskania po awarii powinny powstać jak najszybciej ponieważ zapewniają one kontynuacje funkcjonowania firmy w razie wystąpienia zagrożenia. Integracja oprogramowania AntiVirus wspomoże organizacje w ograniczaniu i wykrywania potencjalnego ryzyka. Aby zabezpieczyć kapitał schowany w fizycznej lokacji Botium Toys należy wprowadzić zamki oraz system CCTV. Systemy o niekrytycznym znaczeniu polecamy wprowadzić przy najbliższej okazji.