Dzień świstaka

czyli jak nie wpaść w pętlę czasu

Wymagania normatywne są często interpretowane z wykorzystaniem analizy słowotwórczej zamiast wiedzy inżynierskiej. Prowadzi to do wielu absurdów, których skutkiem jest fałszywe poczucie bezpieczeństwa bazujące na wypełnionych ex cathedra tabelkach wykazujących zgodność (*compliance*), chociaż zabezpieczenia nie zostały skuteczne wdrożone i nie są właściwie stosowane.

Paweł Henig

absolwent Wydziału Elektroniki Politechniki Warszawskiej. Od połowy lat 90. budował dla centralnej administracji rządowej centra przetwarzania danych i sieci rozległe. Audytor wewnętrzny systemów zarządzania obejmujących normy: zarządzania jakością (ISO 9001), zarządzania środowiskowego (ISO 14001), zarządzania bezpieczeństwem i higieną pracy (OHSAS 18001), bezpieczeństwem produkcji wartościowej (CWA 14641 – Intergraf) oraz zarządzania bezpieczeństwem informacji zgodnie z normą ISO/IEC 27001. Certyfikowany audytor systemów IT (CISA), posiadacz certyfikatu ITIL Foundation. Rzeczoznawca PTI, ekspert PIIT. Dyrektor Operacyjny Trusted Information Consulting Sp. z o.o.

Problemem podstawowym jest brak wiedzy i umiejętności oraz właściwego zorganizowania, czyli przypisania uprawnień i odpowiedzialności osobom, które powinny zaprojektować (Plan), stosować (Do), zweryfikować (*Check*) i ewentualnie skorygować (*Act*) funkcjonowanie systemu zarządzania bezpieczeństwem informacji.

Organy zarządzające najczęściej postrzegają cyberbezpieczeństwo przez pryzmat wymagań prawnych – takich jak KRI, NIS czy DORA – i dlatego powierzają je prawnikom.

Prawnicy, pomimo braku niezbędnej wiedzy z zakresu budowy systemów informatycznych i nadzoru nad technologiami IT (*IT Governence*), mogą uzyskać uprawnieninia audytora wiodącego systemu zarządzania bezpieczeństwem informacji (PN-EN ISO/IEC 27001). Umiejętność pamięciowego przyswajania wiedzy encyklopedycznej jest ich dużym atutem. Tym samym legitymizują oni swoją pozycję wobec organów zarządzających jako ekspertów w zakresie cyberbezpieczeństwa.

Osoby zajmujące się technicznym utrzymaniem systemów posługują się zupełnie innym językiem i często nie rozumieją kwestii zarządczych. Ich zadaniem jest utrzymanie istniejących rozwiązań w sprawności technicznej.

> *Wiedzą, co i gdzie kliknąć, ale niekoniecznie dlaczego.*

Po wdrożeniu systemu zawartość poszczególnych dokumentów projektowych często się dezaktualizuje, bo nikt ich nie utrzymuje. Nie przypisano odpowiedzialności za architekturę systemową i dopasowanie rozwiązań, a cykl ADM (*Architecture Development Method*) pozostaje jedynie w dokumentacji standardu TOGAF. Tę lukę kompetencyjną dobrze widzą audytorzy zewnętrzni, którzy nie zostali zatrudnieni tylko po to, aby za przysłowiową złotówkę „odfajkować" raport zgodności na bazie ładnie wydrukowanej, lecz całkowicie nieadekwatnej i niestosowanej dokumentacji.

Kwestia czasu

Jeżeli w organizacji był wdrażany duży system, to prawdopodobnie obejmował on zagadnienia synchronizacji czasu.

„Zegary systemów przetwarzania informacji wykorzystywanych w organizacji należy zsynchronizować z zatwierdzonymi źródłami czasu" (norma PN-EN ISO/IEC 27001 wymaganie A.8.17. Synchronizacja zegarów).

Na pytanie, czy zegary systemów są zsynchronizowane z reguły usłyszymy odpowiedź – tak. Rzadko dowiemy się, w jaki sposób ta synchronizacja się odbywa, a nad problemem jej istotności nikt się nie zastanawia.

Najczęściej można usłyszeć, że synchronizacja pozwala na powiązanie ze sobą zdarzeń w logach w przypadku wystąpienia incydentu, ale to tylko dla ekspertów. Innych to przecież nie dotyczy (no bo kto ma dostęp do logów, a poza tym kto ma czas je przeglądać!).

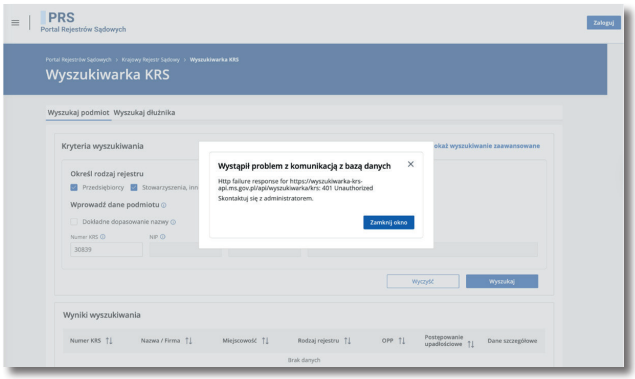
O możliwości wystąpienia problemów z zarządzaniem wątkami i procesami przez jądro systemu praktycznie nikt nie wie. Błękitny ekran śmierci (BSOD) Windows zazwyczaj przypisuje się „jakiejś awarii", a winą obarcza się twórcę systemu (w tym przypadku Microsoft).

Kwestie dostępności systemu związane z wykorzystaniem kryptografii oraz ograniczeniem czasu zaufania do sekretu w takich protokołach jak KERBEROS czy NTLM są wiedzą tajemną. Skoro coś nie zadziałało, to na pewno nie jest to wina żadnej synchronizacji czasu tylko …

Dostęp jest kluczowy

Bez dostępu do informacji biznes po prostu nie działa. Na dokładkę procesy kontroli dostępu, a w szczególności uwierzytelniania, są bardzo powściągliwe w raportowaniu błędów po to, by utrudnić potencjalnemu wrogowi rozpoznanie zabezpieczeń systemu. Przy okazji utrudnia to diagnostykę pozostałym użytkownikom systemu.

Ostatnio pojawił się jeszcze jeden ciekawy przypadek utraty dostępu w związku z brakiem synchronizacji zegarów, który nie jest związany z uwierzytelnianiem ani z przesyłaniem sekretów. Tym razem wykorzystano znakowanie czasem zapytania przesyłanego siecią, aby uchronić bazę danych przed atakiem typu odmowa usługi (DOS). W tym przypadku aplikacja może odrzucić zapytanie złożone „zbyt dawno", czyli ochronić przed atakiem powtórzeniowym (*Reply*) bez sprawdzania zawartości tego zapytania (aby nie obciążać bazy danych). Wystarczy, że zegar systemu, z którego wysłano zapytanie, późni się o kilka sekund i nasze zapytanie zostanie odrzucone. Dostaniemy wtedy taki komunikat:



Możemy spróbować ponownie. Jak bohater filmu „Dzień Świstka" będziemy przeżywali kolejne niepowodzenia, dopóki nie rozwiążemy naszego problemu. Najpierw jednak musimy zrozumieć przyczynę podstawową. Zakończone sukcesem wysłanie zapytania z innego komputera tylko usypia czujność. A problem pozostanie niezależnie od elegancko wypełnionych tabelek zgodności, bo zgodnie z prawem Murphy'ego „jeśli coś może pójść źle, to pójdzie" (najczęściej w najgorszym możliwym momencie).