Bezpieczne korzystanie z narzędzi LegalTech

***Bezpieczne korzystanie z narzędzi LegalTech* to temat kolejnego z cyklu artykułów, zainicjowanych i przygotowanych przez Instytut LegalTech Naczelnej Rady Adwokackiej.**

W ramach działalności Instytutu w każdy piątek w ramach serii "Cyfrowe piątki" na profilach społecznościowych Naczelnej Rady Adwokackiej pojawiają się także posty dotyczące LegalTech, a w szczególności informatyzacji, cyfryzacji i narzędzi wspierających pracę prawnika.

Nie powinno budzić wątpliwości, że korzystanie z narzędzi LegalTech może przynieść istotne korzyści dla prawnika czy to już teraz, czy też w niedalekiej przyszłości. Warto zatem korzystać z dostępnych innowacji, a ostatnimi czasy stało się to w niektórych sytuacjach wręcz konieczne (zdalne rozprawy, dostęp do akt sądowych, dostęp do KRS). Natomiast nawet najprostsze narzędzia LegalTech wymagają dostępu do Internetu i korzystania z urządzeń elektronicznych (komputery, smartfony), co z kolei rodzi potrzebę zwiększania świadomości bezpiecznego korzystania z tych narzędzi.

Jedną z form zdobycia wiedzy na temat cyberbezpieczeństwa jest zapoznanie się ze standardami i dobrymi praktykami w tym zakresie. Jeszcze lepiej, jeżeli są to branżowe standardy i dobre praktyki, gdyż można założyć, że osoby je przygotowujące skupiły się na aspektach, które mogą być charakterystyczne dla danej branży. Najlepiej, jeżeli dokumenty te są aktualne lub regularnie aktualizowane, gdyż poziom zabezpieczeń i zagrożeń zmienia się dynamicznie.

Szukając standardów, które w przystępnej formie pokazują podstawowe wymogi, jakie warto wprowadzić w swojej codziennej praktyce, warto zapoznać się z dokumentami przygotowanymi przez stowarzyszenia prawników. Jednym z takich dokumentów jest przygotowany przez International Bar Association (IBA): ‘Cybersecurity Guidelines By the IBA’s Presidential Task Force on Cybersecurity October 2018. (przyp.1)

W standardach IBA, oprócz części opisowej, można znaleźć tabele, które w przystępnej formie zawierają rekomendacje odnośnie podstawowych zabezpieczeń. W przedmiotowych tabelach została przyjęta pewna gradacja ze względu na wielkość prowadzonej kancelarii. Ma to na celu wskazanie, które usługi w przypadku jednoosobowej kancelarii mogą być tylko zalecane, a w przypadku większej firmy, z większą ilością współpracowników, są już wymagane.

Pośród zamieszczonych tam minimalnych standardów zabezpieczeń dla kancelarii jednoosobowych warto wskazać na konieczność stosowania:

- aktualizacji wykorzystywanego oprogramowania,
- wprowadzenia zabezpieczenia urządzeń końcowych (endpoint protection),
- zabezpieczeń przeglądarek internetowych i wykorzystywanych w pracy skrzynek poczty elektronicznej,
- zabezpieczeń mobilnych urządzeń (smartfony, laptopy).

Pod określeniem aktualizacji wykorzystywanego oprogramowania kryją się m.in. zalecenia dotyczące stosowania: programów antywirusowych w standardzie dla firm (business standard), usług filtrujących otrzymywane wiadomości mailowe, aktualizacji systemów operacyjnych wykorzystywanych do pracy na urządzeniach elektronicznych, usług skanowania automatycznego załączników do poczty. Cześć z tych rozwiązań jest włączona w ustawieniach domyślnych narzędzi stosowanych przez prawników, np. w poczcie elektronicznej. Natomiast zawsze warto zweryfikować, czy następuje to w każdym przypadku.

Pod pojęciem zabezpieczenia urządzeń końcowych kryje się zabezpieczenie używanych sieci Wi-Fi, a

w przypadku korzystania ze zdalnych dostępów stosowanie wirtualnych sieci prywatnych (VPN) i nie stosowania niezabezpieczonych sieci publicznych.

Przy zabezpieczaniu przeglądarek internetowych zalecane jest zastosowanie zabezpieczeń tj. systemy filtrujące sieć zabezpieczające przed pobraniem niechcianych plików lub stosowanie oprogramowania antywirusowego zabezpieczającego także przed zainstalowaniem niechcianego oprogramowania (anti-malwere). W przypadku skrzynek poczty elektronicznej nie zaleca się natomiast korzystania z wersji darmowych.

Przy zabezpieczaniu mobilnych urządzeń zaleca się oddzielnie stosowanie urządzeń do celów służbowych, a oddzielne do celów prywatnych. Najbezpieczniejszym rozwiązaniem jest stosowanie dwóch oddzielnych urządzeń, natomiast w przypadku braku takiej możliwości warto wprowadzić zabezpieczenia, które będą oddzielać dane wykorzystane do pracy od danych prywatnych.

Oczywiście warto zapoznać się z całym dokumentem standardów IBA, gdyż w niniejszym artykule zostały wymienione tylko szczątkowe informacje mające za zadanie wskazanie źródeł wiedzy o cyberbezpieczeństwie.

Należy mieć na uwadze, że stosowanie nawet maksymalnych rekomendacji nie niweluje całkowicie ryzyka, ale może znacznie je zmniejszyć. Nigdy bowiem nie jesteśmy w stanie określić, na którym z zastosowanych zabezpieczeń zatrzyma się potencjalny atak lub które z zagrożeń wykorzystuje określone luki w zabezpieczeniach.

Obecnie trwają prace na standardem cyberbezpieczeństwa przygotowywanym w ramach działalności Instytutu LegalTech przy Naczelnej Radzie Adwokackiej. Niedawno przeprowadzone zostało też szkolenie przez Komisję Aplikacji Adwokackiej Naczelnej Rady Adwokackiej dotyczące cyberbezpieczeństwa w pracy adwokata i aplikanta. Zachęcamy do śledzenia pojawiających się w tym zakresie informacji.

(przyp.1) ***https://www.ibanet.org***


ADWOKATURA
POLSKA
Bezpieczne korzystanie
z narzędzi LegalTech