## Cyberbezpieczeństwo w firmach produkcyjnych – najczęstsze błędy i zagrożenia

Cyberzagrożeniom powinniśmy przeciwdziałać nie tylko zabezpieczając się informatycznie, ale także pod względem prawnym, pod kątem procedur, organizacji, kultury bezpieczeństwa i podnoszenia świadomości pracowników. Konieczne jest kompleksowe podejście, żeby zapewnić skuteczność działań. „Cyberbezpieczeństwo w firmach produkcyjnych – najczęstsze błędy i zagrożenia" było tematem webinarium z cyklu How To? Przemysł 4.0. – technologie, najlepsze praktyki, strategie, realizowanego przez Krajową Izbę Gospodarczą Elektroniki i Telekomunikacji w ramach programu Diginno. Więcej informacji o cyklu na stronie https://kigeit.org.pl/diginno-webinary/. Webinarium poprowadzili: dr inż. Bożena Skibicka, pełnomocnik Spółki mis², Krzysztof Chełpiński, Członek Zarządu, Krajowej Izby Gospodarczej Elektroniki i Telekomunikacji oraz Konrad Makar, aplikant radcowski, specjalista ds. cyberbezpieczeństwa w Kancelarii Radcy Prawnego Tomasz Dauerman. Poniższy artykuł został przygotowany w oparciu o informacje z webinaru.

### Malware, phishing i ransomware

Cyberataki to problem globalny, którego ofiarami coraz częściej stają się także organizacje w Polsce. W 2019 zaatakowanych zostało wiele urzędów gmin, organizacji pozarządowych, a także firmy.

Drugim ważnym pojęciem, które należy na wstępie zdefiniować jest ransomware. Jest to oprogramowanie, którego celem jest szantaż użytkownika. Jego źródło słowne wywodzi się od „ransom" - okup i od „software" - oprogramowanie. W efekcie działania blokuje ono nasze dane. Aby się do nich dostać z powrotem przestępcy domagają się zapłacenia okupu. Phishing oznacza wykradanie, wyłudzanie danych. Polega on raczej na stosowaniu wiedzy socjotechnicznej niż technologii i wykorzystuje słabości ludzkie, opiera się na łatwowierności ofiary, przez którą daje się ona podejść różnym sztuczkom wykorzystywanym przez atakujących.

„Konsekwencje, które niesie za sobą ewentualny atak cybernetyczny to w pierwszej kolejności koszty. Są one bardzo wysokie jeżeli mamy do czynienia z szantażem i wówczas albo musimy zapłacić okup albo ponieść konsekwencje utraty i odtworzenia wążnych, często kluczowych danych firmowych.. Oprócz tych czynników należy uwzględnić także odpowiedzialność cywilną i administracyjną firm i osób zarządzających oraz osobistą odpowiedzialność członków zarządu." – mówi Bożena Skibicka, pełnomocnk mis². Jeżeli w wyniku ataku wyciekły dane osobowe

zobowiązani jesteśmy do poinformowania potencjalnych poszkodowanych. Konieczne jest także podjęcie działań PR, które musimy uruchomić, żeby powstrzymać proces utraty dobrego imienia, ograniczając  w pewnym stopniu poniesione szkody.

**Środki zabezpieczeń przed cyberatakami**

Przyczynami powodzenia cyberataków nie są, jak zwykle się uważa braki technologiczne w zabezpieczeniach systemów IT. One odpowiadają tylko za 17% udanych cyberataków. Nie mniej jednak warto dbać o ten aspekt zabezpieczenia naszych danych.

Główne przyczyny udanych cyberataków leżą w zarządzaniu przedsiębiorstwem. Brak procedur lub ich nieegzekwowanie, co dotyczy zwłaszcza polityki zmiany haseł i aktualizacji systemów informatycznych. Efekty negatywne przynoszą także zaniedbania w dziedzinie monitorowania zagrożeń. Jeżeli systemy do monitorowania nie funkcjonują osoby odpowiedzialne nie mają świadomości o lukach w bezpieczeństwie, podatnościach na zagrożenia, z opóźnieniem dowiadują się, że są atakowani.

„Wiele organizacji nie podchodzi do tego zagadnienia właściwe, w sposób planowy. Często brakuje opracowanego i zatwierdzonego systemu zapewnienia ciągłości działania. Tymczasem systemy informatyczne, jeżeli mają działać w sposób ciągły, muszą mieć zagwarantowane duplikowanie zarówno danych jak i funkcji. Ponieważ każdy komponent systemu informatycznego może ulec awarii, oznacza to, że należy zapewnić ciągłość działania systemów, oprogramowania i sprzętu. Konieczne jest także przygotowanie kadry i gotowych procedur na wypadek, gdyby którykolwiek z elementów tego systemu miał zawieść. W szczególności, jeżeli są to systemy krytyczne z punktu widzenia firmy, pracownicy muszą działać praktycznie automatycznie, w sposób wcześniej przygotowany i przećwiczony.” – zauważa Krzysztof Chełpiński, Członek Zarządu, Krajowa Izba Gospodarcza Elektroniki i Telekomunikacji.

Kolejnym elementem jest zabezpieczanie danych poprzez backup oraz aktualizacja systemów wynikająca w głównej mierze z konieczności załatania luk w ochronie przed możliwymi atakami. Należy pamiętać o tym, że o bezpieczeństwie całego przedsiębiorstwa decyduje jego najsłabszy element. Przestępcy mogą dostać się do naszej organizacji i dokonać ataku korzystając z luk w oprogramowaniu nawet takich urządzeń jak na przykład drukarki.

Niezwykle istotne jest stałe podnoszenie świadomości pracowników. Ustawiczne przypominanie użytkownikom, o tym, że systemy organizacji zawierają dane żywotne z punktu widzenia firmy, a

ich utrata, albo dostęp do systemów przez osoby nieuprawnione może spowodować, że stracą pracę, przyczyni się do zwiększenia świadomości i motywacji pracowników.

Ważnym elementem ochrony przed skutkami cyberataku może być wykupienie odpowiedniej polisy ubezpieczeniowej chroniącej firmę przed finansowymi konsekwencjami incydentów bezpieczeństwa.

**Bezpieczeństwo telepracy**

W czasach epidemii pracownicy często działają zdalnie korzystając z własnego sprzętu. W tym przypadku zasadnym jest przyjęcie jednolitych reguł i rozwiązań w ramach organizacji, które odnosiłyby się do minimalnych standardów, które muszą być spełnione przez sprzęt własny pracowników. Druga ewentualność to praca wyłącznie w oparciu o sprzęt firmowy. W wielu organizacjach znaczna część informacji związanych z wykonywaniem pracy wysyłana jest za pośrednictwem prywatnych telefonów komórkowych. Warto mieć na uwadze, że sporo urządzeń nie posiada żadnych systemów antywirusowych.

„Bardzo często zdarza się, że informacje te wysyłane są przez portale społecznościowe, takie jak np. Messenger na FB, czy WhatsApp. Dlatego, dopóki pracownicy nie uzyskają jasnych i klarownych informacji o tym, że nie jest to zgodne z procedurami bezpieczeństwa organizacji, to nie można spodziewać się, że będą tego świadomi.” – podkreśla Konrad Makar, aplikant radcowski, specjalista ds. cyberbezpieczeństwa, z Kancelarii Radcy Prawnego Tomasza Dauermana.

Wprawdzie pojawiają się wzmianki medialne, że ustawodawca pracuje nad wprowadzeniem rozwiązań do kodeksu pracy, które regulować będą te kwestie, jednak trudno obecnie stwierdzić, kiedy faktycznie wejdą one w życie. Z tego powodu warto zastanowić we własnym zakresie się nad kompleksowym podejściem do problemu i przygotowaniem pewnych wytycznych - na jakich zasadach, w jaki sposób realizowana jest praca zdalna.

**Znaczenie audytu bezpieczeństwa**

Istotnym elementem podnoszenia standardów bezpieczeństwa jest audyt. Dotyczy on zarówno kwestii informatycznych jak i organizacyjno-prawnych. Realizacja każdego audytu powinna zakończyć się sporządzeniem raportu końcowego, czyli pewnego podsumowania przeprowadzonych działań i rekomendacjami, zapewniającymi zwiększenie standardów

bezpieczeństwa w organizacji. Mowa tutaj przede wszystkim o ocenie kompletności posiadanych systemów informatycznych, stwierdzeniu, które z elementów teleinformatycznych są szczególnie ważne dla bezpieczeństwa przedsiębiorstwa i powinny być regularnie testowane z uwagi na ważkość przetwarzanych danych. Ponadto, konieczne jest wskazanie braków w dokumentacji, która ma ująć całą działalność systemów informatycznych, w tym również elementy związane z umowami i ochroną danych osobowych.

**O czym powinny pamietać Zarządy firm?**

Webinaria „How to? Przemysł 4.0. – technologie, najlepsze praktyki, strategie" są częścią programu Diginno mającego na celu przyspieszenie cyfryzacji firm produkcyjnych. Więcej informacji o programie: https://kigeit.org.pl/diginno/

Temat Przemysłu 4.0. będzie kontynuowany podczas FG Time w marcu 2021 (https://fgtime.pl/)

**O Krajowej Izbie Gospodarczej Elektroniki i Telekomunikacji**
KIGEiT powstała w 1992 roku i działa na podstawie ustawy o izbach gospodarczych. Jest organizacją typu not-for-profit, zrzeszającą grupę podmiotów gospodarczych zajmujących się produkcją, handlem, usługami lub pracami naukowo-badawczymi w zakresie lub na rzecz elektroniki, telekomunikacji, informatyki, teleinformatyki, energetyki, elektrotechniki, automatyki przemysłowej, a także audiowizualnych mediów elektronicznych. KIGEiT zrzesza ponad 190 członków, którzy zatrudniają bezpośrednio ponad 58 000 osób i mają przychody na poziomie ponad 68 mld zł rocznie. KIGEiT jest członkiem DigitalEurope, Krajowej Izby Gospodarczej, Polskiego Komitetu Światowej Rady Energetycznej i Klastra 3×20.

**Dalsze informacje:**
Dorota Sapija, Krajowa Izba Gospodarcza Elektroniki i Telekomunikacji
e-mail: dorota.sapija@kigeit.org.pl
tel. 608 03 84 01