INFORMACJA PRASOWA

Szczepionki na cyfrową odporność firm

Warszawa, xx września 2021 – Przed 2019 rokiem tylko nieliczni zdawali sobie sprawę, jak duże znaczenie dla odporności firm na utrudnienia w ich działalności, ma odporność cyfrowa. Dopiero koronawirus pokazał, że technologie cyfrowe mogą pomóc nawet wtedy, kiedy przestaje działać tradycyjna gospodarka. Dziś o poziomie odporności firm na wstrząsy świadczy poziom odporności ich IT. Najważniejsze „szczepionki" na uzyskanie cyfrowej odporności wybrał Jacek Chmiel, dyrektor Avenga Labs, jednostki, która analizuje technologiczne trendy i biznesowe zastosowania innowacji.

Według IDC, 87% europejskich organizacji ma niską odporność cyfrową. Oznacza to, że w razie wystąpienia wydarzeń utrudniających działalność biznesową nie będą one w stanie zaradzić im przy pomocy rozwiązań cyfrowych. Nie będą też mogły wykorzystać zmienionych warunków na swoją korzyść. Wszystkie te firmy potrzebują znacznych usprawnień w zakresie narzędzi i możliwości cyfrowych.

W Polsce, mimo szybszego niż przed pandemią rozwoju gospodarki cyfrowej, może być jeszcze gorzej niż w całej Europie, ponieważ zapóźnienia dotyczą samej cyfryzacji. Jak podaje GUS, w 2020 roku – już po pierwszej fali pandemii – zaledwie co czwarta firma zatrudniająca co najmniej 10 osób kupowała jakieś usługi w chmurze (niemal 60% spośród dużych firm). Tylko co czwarte takie przedsiębiorstwo zatrudniało specjalistów od ICT (ponad 80% jeśli chodzi o duże firmy).

– *Myślenie o cyfrowej odporności na razie pojawia się głównie w nielicznych, najbardziej zaawansowanych technologicznie firmach. One już traktują IT jako integralną część biznesu. CTO/CIO wchodzą do zarządów, umacniają swoją rolę w biznesie. Od nich coraz bardziej zależy działanie firmy. Od nich oczekuje się też inicjatywy. Zanikają dawne linie podziałów, a równocześnie rośnie znaczenie odporności. Szczęście prowadzenia biznesu w spokojniejszych czasach jest chyba za nami. Myślenie życzeniowe na pewno nie wystarcza. Potrzebne jest działanie* – uważa Jacek Chmiel i wskazuje na 7 głównych elementów cyfrowej odporności:

Avenga – Transforming Industries

Avenga IT Professionals
ul. Przyokopowa 26 (Proximo II)
01-208 Warszawa

www.avenga.com

Kontakt:

Andrzej Godewski
+48 888 651 564
andrzej.godewski@avenga.com

Odporność infrastruktury, którą uzyskuje się poprzez odpowiedni dobór sprzętu i oprogramowania oraz współpracę z wiarygodnymi firmami świadczącymi usługi IT. Ciągłość pracy zwiększa się dzięki redundancji, monitorowaniu i ostrzeganiu w czasie rzeczywistym oraz zautomatyzowaniu działań naprawczych.

Odporność na bankructwa i nierzetelność dostawców oprogramowania opiera się na zasadzie, że prawie zawsze istnieje inny dostawca, oferujący rozwiązania o podobnych możliwościach. Najlepiej korzystać z kilku dostawców lub poprzez system kar i wywieranie presji egzekwować warunki umowy z tym jedynym.

Odporność na zewnętrznych dostawców nie pozwala żadnemu z nich przejąć całkowitej kontroli nad projektami. Jedną z kluczowych kwestii jest własność kodu i prawa do kontynuowania pracy nad tą samą bazą kodów u innego dostawcy lub w ramach wewnętrznego software house'u.

Odporność danych zapewnia stały dostęp do danych, nawet w przypadku awarii rozwiązań typu SaaS. Redundantne pamięci masowe, klastry silników bazodanowych itp., to elementy ekosystemu danych, które wspierają jego odporność.

Odporność na starzenie się technologii pomoże uniknąć sytuacji, w której ze względu na zależność od starszych technologii firma nie będzie w stanie utrzymywać lub rozwijać swoich rozwiązań cyfrowych. Aby zminimalizować to ryzyko, zawsze lepiej stawiać na najpopularniejsze technologie w danej dziedzinie.

Odporność na utratę wiedzy, która znika np. wraz z odejściem z firmy kluczowych specjalistów. Tej odporności nabiera się poprzez pilnowanie, żeby pracownicy zawsze wyjaśniali, dokumentowali swoje prace i regularnie dzielili się wiedzą, szczególnie wtedy gdy jest związana z bazami kodu, konfiguracjami i wdrożeniami.

Odporność w chmurze polega m.in. na zastosowaniu architektur chmury natywnej (Kubernetes, Docker), które sprawdzają się w chmurach hybrydowych, równoważąc różne publiczne chmury i lokalne infrastruktury. Gdy niektóre z węzłów lub całe klastry zawiodą, ruch zostanie przeniesiony do innego węzła lub klastra w innej chmurze lub serwerowni, utrzymując płynność działania.

Generalnie cyfrowa odporność lubi standardy, przewidywalność i jednolitość. Dlatego odporna firma musi oprzeć się na procedurach. Pomaga to w automatyzacji większości typowych scenariuszy i pozwala

Avenga – Transforming Industries

Avenga IT Professionals
ul. Przyokopowa 26 (Proximo II)
01-208 Warszawa

www.avenga.com

Kontakt:

Andrzej Godewski
+48 888 651 564
andrzej.godewski@avenga.com

specjalistom skupić się na poszukiwaniach i innowacjach również w obszarze odporności. Poza tym w odpornych firmach dużą wagę przywiązuje się do dokładnego testowania i obserwowalności rozwiązań IT. W tworzeniu oprogramowania wykorzystuje się architekturę ewolucyjną, z natury wspierającą ciągłe zmiany.

Punktem wyjścia na drodze do cyfrowej odporności jest zdefiniowanie jej oczekiwanego poziomu. Docelowo cyfrowa odporność powinna stać się elementem proaktywnej strategii zarządzania ryzykiem w IT. Kluczem jest znalezienie właściwej równowagi pomiędzy eksperymentowaniem i innowacyjnością a odpornością. W każdej firmie będzie ona uzyskana inaczej.