

Minimalizacja ryzyka w przemyśle

Istnienie najskuteczniejszych nawet rozwiązań prewencyjnych nic nie da, jeżeli po stronie przedsiębiorcy nie będzie świadomości ryzyka oraz woli podejmowania działań zapobiegających jego materializacji. – **BARTŁOMIEJ BARTCZAK, MARTA MEISNER**

Działając w obszarze zarządzania ryzykiem, bardzo często poruszamy się na styku interesów zakładów przemysłowych i ubezpieczycieli, z natury rzeczy oscylujących wokół działań mających na celu zapobieżenie materializacji ryzyk związanych z prowadzeniem danej działalności. Na podstawie naszych obserwacji i doświadczeń przedstawiamy 6 trendów, które obecnie najsilniej zaznaczają się w sferze ubezpieczeniowej polityki prewencyjnej dla branży przemysłowej.

WZROST ZNACZENIA INŻYNIERII RYZYKA

Obserwujemy silny trend wśród liderów rynku ubezpieczeniowego do tworzenia komórek wyspecjalizowanych w zakresie analizy ryzyk związanych z działalnością przemysłową i likwidacji największych szkód. W Polsce takie dedykowane zespoły inżynierów mają już Ergo Hestia w postaci spółki Hestia Loss Control, PZU, które stworzyło PZU Lab, czy InterRisk korzystający z usług należącej do grupy VIG firmy Risk Consult. Położenie nacisku na profesjonalne i prowadzone na coraz większą skalę audyty ryzyk sprzyja bardziej świadomemu przyjmowaniu do ochrony i kwotowaniu stawek przez ubezpieczycieli, a także pozwala zoptymalizować ochronę ubezpieczeniową. W szczególności cenną wartość dodaną dla klienta stanowią rekomendacje inżynierów ryzyka, którzy swoje bogate doświadczenie budują, audytując różne spółki (w tym zagraniczne) oraz analizując zdarzenia szkodowe.

Coraz częściej ubezpieczyciele we wspólnym interesie – zapewnienia bezpieczeństwa sobie i klientowi – decydują się też oferować lub finansować usługi dodatkowe – w tym badania nieniszczące. **Budowanie przewagi konkurencyjnej przez ubezpieczycieli w oparciu o identyfikację ryzyk i rekomendowanie działań prewencyjnych jest inicjatywą, która spotyka się z dużym zainteresowaniem przedstawicieli przemysłu z uwagi na ogólne korzyści.**



Bartłomiej Bartczak
jest wiceprezensem
Risk Coach Lab.

LEPSZE WYKORZYSTANIE DANYCH DZIĘKI NOWOCZESNEJ TECHNOLOGII

Podstawą skutecznego zastosowania działań prewencyjnych jest ich dostosowanie do warunków danej działalności – zatem kluczowe znaczenie mają informacje płynące z samego przedsiębiorstwa, w szczególności te pozwalające wychwycić trendy i anomalie. Duże zakłady przemysłowe są jednak generatorami gigantycznej ilości szybko zmieniających się danych, w przypadku których analiza i obróbka, a następnie wnioskowanie na ich podstawie nie jest zadaniem prostym. Optymalizacja tych procesów jest coraz częściej prowadzona przy zastosowaniu nowoczesnych technologii, takich jak metodologia analizy sieci big data, która umożliwia wyselekcjonowanie z olbrzymich baz danych informacji najbardziej istotnych. Bardzo obiecujące jest wdrażanie do przemysłu innowacyjnych technik *data miningu*, tj. eksploracji danych bazującej w szczególności na statystyce i uczeniu maszynowym. Popularność zyskuje też analityka predykcyjna, która – wykorzystując dane bieżące i historyczne – pozwala identyfikować zagrożenia i prognozować awarie. Jej wykorzystanie dla celów predykcyjnego utrzymania ruchu jest nowoczesną strategią zarządzania eksploatacją urządzeń ukierunkowaną na niezawodność oraz gotowość zadaniową. **Zastosowanie w przemyśle skutecznej prognozy zapewniającej optymalne użytkowanie maszyny i wykluczenie pojawienia się awarii wydaje się idealnym modelem prewencji, który coraz bardziej doceniają przedsiębiorcy i ubezpieczyciele.**



Marta Meisner
jest specjalistą
w Risk Coach Lab.

Pamiętajmy jednak, że – poza samym zaimplementowaniem technologii pozwalających analizować dane – warunkiem koniecznym do uzyskania pożądanego efektu prewencyjnego jest pozyskiwanie odpowiednich informacji. Dlatego kluczową rolę odgrywa opomiarowanie instalacji przemysłowych, co niestety często niesie ze sobą znaczące koszty. Jest to jednak wydatek, który przedsiębiorcy decydują się coraz częściej ponosić, mając świadomość korzyści, jakie płyną z dobrego wykorzystania danych na potrzeby zwiększenia bezpieczeństwa oraz zapewnienia optymalności i ciągłości funkcjonowania, co z kolei przekłada się na budowanie przewagi konkurencyjnej.

INNOWACYJNE METODY ZWIĘKSZENIA BEZPIECZEŃSTWA

W celu minimalizacji ryzyka ubezpieczeniowego w przemyśle w ostatnim czasie bardzo duży nacisk jest kładziony na wdrażanie rozwiązań zwiększających funkcje bezpieczeństwa dotychczas istniejących obiektów, jak również optymalizację projektowania rozbudowy przedsiębiorstwa z wykorzystaniem innowacyjnych rozwiązań.

Silnym trendem jest coraz szersze wykorzystywanie dronów, m.in. na potrzeby kontrolowania granic przedsiębiorstwa czy np. stanu urządzeń, w tym ewentualnych uszkodzeń, które znajdują się na znacznej wysokości lub na bardzo dużej przestrzeni (np. linie przesyłowe). Nie ulega wątpliwości, że wkrótce liczba zastosowań tych latających urządzeń na potrzeby zwiększenia bezpieczeństwa działalności zakładów

PREWENCJA

przemysłowych znacznie wzrosnąć. Obraz pozyskany m.in. przy pomocy dronów może znaleźć zastosowanie np. na potrzeby technologii modelowania 3D zakładu. Model 3D pozwala na uporządkowanie, usystematyzowanie i digitalizację kluczowej infrastruktury przemysłowej, jednocześnie tworząc pełną inwentaryzację na potrzeby ubezpieczeniowe. W przypadku zajścia zdarzenia szkodowego ułatwia w znacznym stopniu wykazanie stanu faktycznego przed zajściem zmian, co pozwala wykluczyć ewentualne wątpliwości, tym samym przyspieszając proces likwidacji szkody.

Kolejnym ciekawym rozwiązaniem jest implementowanie w ramach instalacji przemysłowych systemów monitorowania różnego rodzaju. Przykładem może być system monitorowania skuteczności wypełniania funkcji bezpieczeństwa przez zainstalowane na obiekcie systemy bezpieczeństwa, łącznie z monitorowaniem efektywności czynnika ludzkiego. Nadzrędnym celem tego systemu jest zapewnienie nieprzerwanej dostępności zdolności produkcyjnych i funkcjonowania przedsiębiorstwa na akceptowalnym poziomie bezpieczeństwa.

Inny model monitoringu można zastosować w celu kontroli diagnostycznej stanu urządzeń technicznych w trakcie ich eksploatacji przy wykorzystaniu bezinwazyjnej metody emisji akustycznej, która umożliwia wykrycie oraz zlokalizowanie wad materiałowych lub innych defektów różnego rodzaju obiektów, w tym np. zbiorników, rurociągów, konstrukcji betonowych i stalowych oraz żelbetowych, urządzeń energetycznych, poszycia kadłubów statków lub samolotów, urządzeń wydobywczych. Wyniki tych badań są niezwykle przydatne w celu podjęcia działań wyprzedzających i planowania remontów, gwarantując jednocześnie bezpieczeństwo eksploatacji oraz optymalizację kosztów napraw.

Przedstawione rozwiązania są dla ubezpieczycieli bardzo interesujące z uwagi na ich zastosowanie w celach prewencyjnych, czego naturalnym efektem jest coraz częstsze nawiązywanie przez zakłady ubezpieczeń relacji biznesowych z dostawcami tego typu technologii czy wręcz inwestowanie w takie innowacyjne rozwiązania.

ZORIENTOWANIE NA CYBERBEZPIECZEŃSTWO

Poza zagrożeniami związanymi z funkcjonowaniem w sieci, takimi jak utrata danych czy cyberwymuszenia, uwaga ubezpieczycieli, menedżerów ryzyka i spoleczeństwa w coraz większym stopniu skupia się na zagrożeniu

cyberatakami na przemysłowe systemy sterowania, które mogą doprowadzić do szkód w mieniu i w środowisku, a nawet konsekwencji dla zdrowia i życia ludzi.

Przeprowadzone w ostatnich latach w naszym rejonie ataki tego typu (np. wynikające z cyberataków: przejęcie kontroli nad stalownią w hucie Hochofen w Niemczech, wybuch ropociągu Baku – Tiblisi – Ceyhan czy odcięcie zasilania w energię elektryczną na Ukrainie) są traktowane jako działania terrorystyczne i nie pozostawiają złudzeń co do realności tego zagrożenia oraz potencjalnie katastroficznych konsekwencji.

O aktualności i randze tematyki cyberbezpieczeństwa w przemyśle świadczy także przyjęcie przez Parlament Europejski dyrektywy w sprawie bezpieczeństwa sieci i informacji w obrębie Unii Europejskiej (NIS), która szczególnie obowiązkowo wdrażania działań zwiększających bezpieczeństwo i raportowania incydentów nakłada na operatorów infrastruktury krytycznej (w tym podmioty z branży energetyki i transportu). Obecnie następuje otwarcie się ubezpieczycieli na ryzyka cybernetyczne, które wcześniej w większości były wyłączone z udzielanej ochrony, przy jednoczesnym oferowaniu usług dodatkowych mających na celu minimalizację cyberzagrożeń lub ograniczenie skutków ataków. W obszarze cyberbezpieczeństwa obsługa przedsiębiorstw przez zakłady ubezpieczeń powinna mieć charakter kompleksowy – w uzupełnieniu produktów ubezpieczeniowych musi obejmować też usługi prewencyjne, takie jak: wykrywanie podatności na cyberatak, stały monitoring systemów czy tworzenie planów ciągłości działania pod kątem zagrożeń cybernetycznych. Zasadniczy nacisk trzeba również położyć na jakość i szybkość usług assistance na wypadek wystąpienia cyberataku, które powinny być prowadzone przez wysoko wykwalifikowaną kadrę złożoną w szczególności z informatyków i prawników.

ZWIĘKSZANIE NIEZAWODNOŚCI PRACOWNIKÓW

Niezawodność człowieka jest istotnym czynnikiem niezawodności układów technicznych, a – jak wskazują badania – błąd ludzki jest przyczyną 30–70% awarii. Oczywiście niezawodność pracownika jest szczególnie ważna w zawodach i na stanowiskach charakteryzujących się znaczną zmiennością warunków pracy, ponadprzeciętnymi umiejętnościami oraz tam, gdzie zawodność człowieka prowadzi do znaczących konsekwencji. Takie warunki pracy często panują w dużych zakładach przemysłowych,

w których błąd ludzki może doprowadzić do wielkich szkód w ludziach i mieniu (np. w wyniku wybuchu), szkód w środowisku (np. wskutek wycieku substancji niebezpiecznej) czy strat finansowych (np. w efekcie wstrzymania funkcjonowania zakładu). Dlatego też **niezwykle ważnym elementem prewencji ubezpieczeniowej jest cykliczne szkolenie operatorów kluczowych instalacji.** Mając na uwadze, że człowiek zapamiętuje tylko 10% tego, co przeczyta, 50% tego, co usłyszy i zobaczy, a aż 90% tego, co robi – szczególnie dobre efekty przynoszą szkolenia kadry na funkcjonujących instalacjach, co jest jednak często bardzo trudne lub wręcz niemożliwe. Dlatego też rośnie zainteresowanie symulatorami, które umożliwiają prowadzenie szkoleń w warunkach zbliżonych do rzeczywistych, w szczególności w warunkach występowania zagrożeń na „funkcjonującym obiekcie”. Symulatory mogą odwzorowywać systemy sterowania, na jakich operują pracownicy, lub pozwalać na poruszanie się pracownika po wirtualnym obiekcie i interakcję z urządzeniami czy innymi pracownikami. W naszej opinii symulatory szkoleniowe będą w najbliższym czasie intensywnie rozwijane jako wyjątkowo skuteczne narzędzie budowania niezawodności pracowników i niewątpliwie tego typu inicjatywy spotkają się z poparciem branży ubezpieczeniowej.

BUDOWANIE KULTURY BEZPIECZEŃSTWA

Nie jest niczym odkrywczym, że istnienie najskuteczniejszych nawet rozwiązań prewencyjnych nic nie da, jeżeli po stronie przedsiębiorcy nie będzie świadomości ryzyka oraz woli podejmowania działań zapobiegających jego materializacji. Obserwowane już od lat zjawisko budowania kultury bezpieczeństwa, do którego w znacznej mierze przyczynia się także branża ubezpieczeniowa, pozostaje nadal aktualne. Co prawda, świadomość co do konsekwencji wystąpienia szkód i korzyści płynących z zapobieżenia im rośnie z każdym rokiem, w firmach coraz częściej zatrudniani są wykwalifikowani menedżerowie ryzyka, a poaudytowe rekomendacje ubezpieczycieli nie są od razu chowane do szuflady, jednak w obliczu nieustannie pojawiających się nowych zagrożeń oraz dynamicznie zmieniających się możliwości i, co istotne, kosztów działań zapobiegawczych – rozmawianie o ryzyku i prewencji, prowadzenie szkoleń w tym zakresie oraz szukanie nowych rozwiązań istniejących problemów powinno być nadal priorytetem zarówno branży ubezpieczeniowej, jak i przemysłu. □