EUROPEAN
RENTAL
ASSOCIATION

STRESZCZENIE

Przewodnik ERA po wiodących praktykach w zakresie bezpieczeństwa cybernetycznego w branży wynajmu sprzętu

Cyberbezpieczeństwo - czy jesteś przygotowany na wyzwania?

Jednym z największych zagrożeń dla branży wynajmu sprzętu jest podatność na wpływ cyberbezpieczeństwa na nasze firmy. W 2021 r. w naszej branży nie ma ustalonej mapy drogowej, na podstawie której firma wynajmująca sprzęt mogłaby ocenić swoją sytuację w odniesieniu do bezpieczeństwa cybernetycznego i określić wiodące praktyki, do których może dążyć. Celem niniejszego Przewodnika jest zdefiniowanie zakresu interwencji związanych z cyberbezpieczeństwem w skali całej firmy, określenie podstawowych elementów skutecznej strategii, w tym szczególnych czynników, które mogą mieć wpływ na firmy wynajmujące, a także nakreślenie wiodących praktyk przyjmowanych obecnie przez liderów w naszej branży. Niniejszy Przewodnik został opracowany dzięki nieocenionemu wsparciu i wkładowi firm członkowskich ERA.

Dzisiejsze zagrożenie związane z cyberbezpieczeństwem i "wezwanie do działania"

W niniejszym Przewodniku przedstawiono, w jaki sposób sektor wynajmu sprzętu w całej Europie stoi w obliczu bezprecedensowego wyzwania, jakim są zagrożenia wynikające z podatności i narażenia na ataki technologii informatycznych w naszej działalności, a w szczególności, w jaki sposób klienci wymagają od nas coraz więcej w zakresie ochrony cyberbezpieczeństwa. W branży trwa proces konsolidacji, w ramach którego mniejsze firmy łączą się z innymi w celu osiągnięcia skali, a większe firmy przejmują mniejsze, aby wejść na nowe rynki, skonsolidować się lub zdobyć udział w rynku. Branża wynajmu sprzętu przechodzi "cyfryzację". Więcej online oznacza więcej zagrożeń cyberbezpieczeństwa. Sprzęt przeznaczony do wynajmu staje się coraz bardziej inteligentny i podłączony do sieci, co może być przepustką do ataku. Firmy zajmujące się wynajmem sprzętu, które doświadczyły poważnego incydentu, mają poczucie, że naraziły na wysokie ryzyko swoją działalność, reputację, a przede wszystkim swoich klientów i interesariuszy. Prawodawstwo UE staje się coraz bardziej intensywne, a Przewodnik wskazuje na najnowsze zmiany w dyrektywie UE NIS (Security of Network and Information Technology - Dyrektywa w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych). Branża potrzebuje obecnie stałej społeczności wśród firm europejskich, która będzie współpracować w zakresie najlepszych praktyk dotyczących bezpieczeństwa cybernetycznego, wspólnych zagrożeń i problemów, z którymi borykają się wszystkie organizacje.

Budżetowanie w zakresie cyberbezpieczeństwa i potrzeby inwestycyjne

Niniejszy Przewodnik przedstawia inwestycje i koszty związane z zapewnieniem bezpieczeństwa cybernetycznego. Przedstawia on skalę inwestycji i "dojrzałości", wskazując początkowe nakłady na wprowadzenie podstaw. Dobre cyberbezpieczeństwo wymaga znacznych inwestycji - i musi być co roku odnawiane. Bezpośrednie inwestycje w cyberbezpieczeństwo we wszystkich branżach są szacowane na około 5% wydatków na IT, przy czym na początku jest to więcej. Liderzy wskazują również, że większą inwestycją są pośrednie i niematerialne koszty "projektowania", zarządzania i wbudowywania bezpieczeństwa we wszystko, co robią, które ostatecznie mogą wynieść więcej niż koszty bezpośrednie.

Mapa drogowa wiodących praktyk i "lista kontrolna"

Interwencje w zakresie cyberbezpieczeństwa często koncentrują się wokół technologii i systemów, jednak wiele zagrożeń ma swoje źródło w zachowaniach ludzkich, solidności procesów oraz monitorowaniu, raportowaniu i reagowaniu w przedsiębiorstwie. Według liderów wynajmu sprzętu w tej dziedzinie, organizacja musi rozważyć strategię obejmującą całe przedsiębiorstwo, aby zapewnić, że wszystkie obszary podatności na zagrożenia są brane pod uwagę. Każda organizacja będzie miała inne ryzyko, zakres działania i luki, jednak Liderzy uważają, że lista kontrolna dla kompleksowego zakresu może być ujęta w czterech elementach zdolności obejmujących Proces, Ludzi, Technologię i Infrastrukturę, dlatego też niniejszy Przewodnik analizuje je i przedstawia podstawowe wymagania dotyczące zdolności na każdym z trzech poziomów: "Poziom Podstawowy", "Dojrzewanie" i "Lider". Do przewodnika dołączona jest lista kontrolna, która łączy zasadniczą ocenę ryzyka i podatności z aktualnym poziomem dojrzałości firmy jako pomoc w planowaniu i redukcji ryzyka.

"*Dostajesz to, co mierzysz …..”* Wiodące firmy twierdzą, że konieczne jest zapewnienie, aby kluczowe obszary działania, które mają wpływ na stan bezpieczeństwa cybernetycznego, były oceniane za pomocą Kluczowych Wskaźników Efektywności (KPI). Mapa drogowa zawarta w przewodniku wskazuje typowe środki i systemy pomiaru efektywności stosowane obecnie przez wiodące firmy dla każdego z elementów.

Przykłady najlepszych praktyk

Niniejszy Przewodnik ilustruje niektóre z wiodących praktyk stosowanych obecnie w odniesieniu do czterech elementów potencjału. Liderzy podkreślają, że chociaż kompleksowy plan bezpieczeństwa stanowi istotną część kompleksowej strategii, to jednak nie musi być pierwszym krokiem - pełny plan może być zazwyczaj realizowany w etapach dojrzałości. Kluczowe cechy obejmują:

- **Proces**: Wiodące firmy podkreślają, że na wczesnych etapach ważniejsze jest podjęcie kroków w celu zidentyfikowania wszystkich możliwych obszarów wysokiego ryzyka w firmie oraz ustalenie priorytetów działań mających na celu wyeliminowanie lub poprawienie słabych punktów. Dobrym punktem wyjścia może być kompleksowe badanie ryzyka w każdym z podstawowych obszarów niniejszego przewodnika. Po uporaniu się z obszarami wysokiego ryzyka, można zająć się obszarami średniego ryzyka. Należy zaznaczyć, że badania wskazują, iż przejście od poziomu podstawowego do objęcia wszystkich istotnych obszarów ryzyka może być procesem trwającym od trzech do pięciu lat, wymagającym istotnych i trwałych inwestycji. Liderzy wskazują na podstawowy, lepszy i najlepszy rodzaj procesu prowadzącego do osiągnięcia bezpieczeństwa dostosowanego do celu, który może wykorzystywać formalne akredytacje jako kamienie milowe lub być budowany na zamówienie w firmie i opierać się na tych samych zasadach. Przedstawiono szereg międzynarodowych ramowych wytycznych, które są w użyciu.

- **Ludzie:** *Cyberbezpieczeństwo to nie "sprawa IT”…* W obronie cyberbezpieczeństwa ważną rolę odgrywa zarządzanie zasobami ludzkimi (HR). Zakres interwencji i wsparcia działu zarządzania zasobami ludzkimi w wiodących firmach jest szeroki i obejmuje projektowanie i opracowywanie polityk i procedur (w tym RODO i protokołów ochrony danych) oraz przekazywanie ich wszystkim pracownikom, dostosowywanie warunków zatrudnienia i opisów ról w celu uwzględnienia obowiązków związanych z danymi i bezpieczeństwem, podnoszenie świadomości i szkolenie w zakresie wymogów cyberbezpieczeństwa oraz analizę potrzeb szkoleniowych dla pracowników pierwszej linii i personelu odpowiedzialnego za bezpieczeństwo. Niezbędne są środki komunikacji, takie jak biuletyny informacyjne lub biuletyny w mediach społecznościowych, służące do informowania o najnowszych trendach lub zagrożeniach w całym przedsiębiorstwie.

- **Technologia:** Narzędzia informatyczne wciąż szybko się rozwijają i zapewniają potężne środki obrony cybernetycznej, służące do "wczesnego ostrzegania" i przechwytywania zagrożeń. Monitorowanie zagrożeń i stanu infrastruktury jest możliwe dzięki technologii z zaawansowanymi systemami, takimi jak "Splunk" i "MS Azure Sentinel", przedstawionymi na ilustracjach w użyciu. Ustanowienie "SOC" (Security Operations Centre - Centrum Bezpieczeństwa Operacyjnego) jest pokazane jako niezbędne, aby w pełni wykorzystać możliwości zautomatyzowanych systemów. Wiodące firmy mogą prowadzić wewnętrzne SOC, często uzupełniane przez zewnętrzne centra, które mogą oferować wsparcie 24x7 oraz zaawansowane usługi monitorowania i zarządzania.

- **Infrastruktura:** *"Jeśli pomimo wszystkich najlepszych środków zapobiegawczych wydarzy się najgorsze, trzeba mieć przygotowany Plan Zarządzania Incydentem".* Ataki mogą przybierać różne formy, ale jednym z najpoważniejszych jest atak typu "ransomware". W sytuacji odmowy dostępu do systemów konieczna jest natychmiastowa reakcja kryzysowa, ale należy wdrożyć proces oceny i "segregowania" sytuacji. Niniejszy Przewodnik ilustruje, w jaki sposób wiodące firmy analizują i reagują, a także przedstawia szablon "pierwszych 48 godzin", który może pomóc w zaplanowaniu okresu zarządzania kryzysowego bezpośrednio po wystąpieniu zdarzenia odmowy dostępu do systemów lub innego poważnego zagrożenia awarią.

Przygotuj się na bezpieczną przyszłość

Wysiłki na rzecz bezpieczeństwa IT nigdy się nie skończą, ale aby pozostać w czołówce, wiodące firmy podkreślają, że wypożyczalnie sprzętu muszą:

1. *Znać swoje zasoby, mocne i słabe strony*
2. *Przeprowadzać ocenę ryzyka*
3. *Odpowiednio planować i inwestować*
4. *Być przygotowanym na wypadek, gdyby stało się najgorsze*
5. *Stale aktualizować i doskonalić swoją wiedzę*

"Przewodnik ERA po wiodących praktykach w zakresie bezpieczeństwa cybernetycznego" ma na celu pomóc firmom zajmującym się wynajmem sprzętu wszelkiego rodzaju i wielkości w planowaniu, rozwijaniu i ciągłym doskonaleniu cyberbezpieczeństwa.