



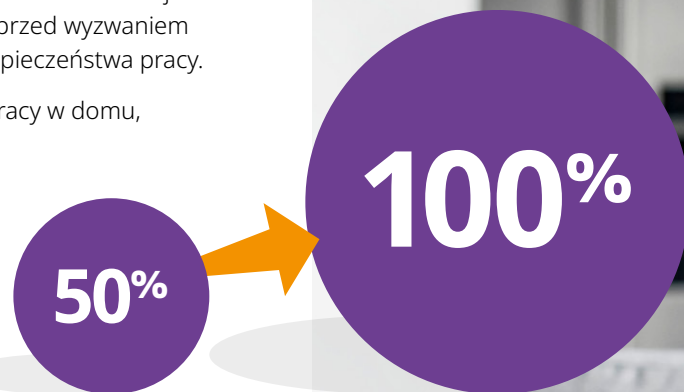
Zadbaj o bezpieczeństwo swojej firmy, gdy wymagana jest praca zdalna

Dyrektor ds. bezpieczeństwa Informacji w firmie Alcatel-Lucent Enterprise, Sebastien Roche, dzieli się swoimi spostrzeżeniami na temat podejścia ALE do ciągłości działania i bezpieczeństwa w tych trudnych czasach

Nowa rzeczywistość #WFH

W związku z niedawnym międzynarodowym kryzysem zdrowotnym i wprowadzonymi na całym świecie działaniami dotyczącymi pozostania w domu, firmy, które wcześniej nie oferowały opcji pracy w domu (#WFH – ang. work from home), stają przed wyzwaniem przekształcenia swoich organizacji w celu zapewnienia ciągłości i bezpieczeństwa pracy.

W 2008 roku firma Alcatel-Lucent Enterprise zainicjowała strategię pracy w domu, którą przyjęło ponad 50% z 2000 pracowników pracujących w 50 biurach na całym świecie. Ponieważ ponad połowa pracowników Alcatel-Lucent Enterprise pracuje w domu, posiadaliśmy już sieć i architekturę IT niezbędną do obsługi pracy zdalnej. Prawdziwym wyzwaniem było przejście z 50% pracowników wykonujących pracę online do 100%.



Gotowość do działania

W ciągu trzech lat poprzedzających niedawny kryzys w służbie zdrowia firma Alcatel-Lucent Enterprise rozpoczęła szeroko zakrojoną transformację infrastruktury IT. Zaadoptowano architekturę sieci WAN zdefiniowaną przez usługę, która zapewniła bezpieczeństwo w chmurze w celu aktywnego blokowania wątków, identyfikacji potencjalnych ataków i zapewnienia bezpiecznego dostępu dla pracowników.

Transformacja ta obejmowała:

- Bezpieczeństwo w chmurze dzięki wirtualnym punktom dostępowym
- Śledzenie w czasie rzeczywistym
- Identyfikowanie nietypowych wzorców zachowań w celu wykrywania zagrożeń



Broszura

Zadbaj o bezpieczeństwo swojej firmy, gdy wymagana jest praca zdalna





Przygotowanie = szybkie reagowanie w sytuacjach kryzysowych

Decyzja o rozpoczęciu pracy zdalnej w poniedziałek została podjęta w poprzedni piątek po południu. Pracownicy zostali poinstruowani, aby zabrać ze sobą laptopy i monitory do domu. W poniedziałek rano praca rozpoczęła się jak zwykle, bez zakłóceń, ponieważ pracownicy zaczęli dzień w swoich zdalnych biurach. Przeprowadzona wcześniej transformacja sieci zapewniła bezpieczną łączność zdalną, niezależnie od ich lokalizacji.

Wyzwanie związane z dostępem

Jednym z głównych wyzwań, przed którymi stanęliśmy, były profile użytkowników, w tym zespoły badawczo-rozwojowe i wsparcia technicznego, posiadające określone potrzeby dostępu do niektórych serwerów i platform programistycznych, na co nie pozwalało nasze rozwiązanie dostępu zdalnego. Te pracownicze profile użytkowników zostały przekazane przez inne dedykowane rozwiązania dostępu niż w przypadku pozostałych zespołów.

Wraz z rozpoczęciem działań mających na celu przeniesienie wszystkich pracowników do trybu #WFH, dostosowaliśmy naszą infrastrukturę, aby zwiększyć przepustowość i móc obsłużyć wzrost liczby połączeń zdalnych wymaganych przez pracowników zdalnych.

Bezpieczeństwo to podstawa

Bezpieczeństwo i ochrona danych przedsiębiorstwa są niezwykle ważne w tych niepewnych czasach i mają wpływ na wiele organizacji obsługujących dane wrażliwe, takich jak organizacje sektora publicznego, ministerstwa, miasta i miasteczka.

Jeszcze zanim zaczęliśmy rozmowy o #WFH w ALE, wdrożyliśmy rozproszoną i zabezpieczoną infrastrukturę, a także w pełni oparte na chmurze rozwiązanie do połączeń prywatnych dla wszystkich pracowników, aby zapewnić bezpieczny zdalny dostęp do sieci. Utrzymywaliśmy dotychczasowe rozwiązanie VPN dla niewielkiego odsetka zespołów, które miały określone potrzeby, takie jak podłączanie telefonów IP w swoich zdalnych biurach. Zapewniliśmy również pracownikom profesjonalne komputery PC z możliwością zarządzania automatycznym pobieraniem i aktualizacjami oprogramowania.

Broszura

Zadbaj o bezpieczeństwo swojej firmy, gdy wymagana jest praca zdalna

Blokada dostępu w przypadku naruszenia bezpieczeństwa

Zgodnie z oczekiwaniami, w okresie intensywnej pracy zdalnej nastąpił wzrost liczby telefonów i e-maili dotyczących podejrzanych wiadomości e-mail oraz próśb o aktualizację haseł. Odnotowaliśmy również wzrost liczby ataków phishingowych, a także ataków ukierunkowanych na podatne oprogramowanie.

Podczas gdy korzystanie z serwerów proxy chroni firmę Alcatel-Lucent Enterprise przed poważnymi problemami związanymi z bezpieczeństwem cybernetycznym, codziennie obserwujemy nowe naruszenia, których źródłem są wiadomości e-mail, pobrania lub brak aktualizacji wersji oprogramowania/systemu operacyjnego.

Utrzymywanie otwartej komunikacji

W tym trudnym okresie utrzymujemy stały, wirtualny kontakt z zespołami Alcatel-Lucent Enterprise. Regularnie komunikujemy się, dzielimy się wskazówkami i najlepszymi praktykami oraz zapewniamy, że nasz zespół jest dostępny dla wszystkich pracowników.

Lista kontrolna Alcatel-Lucent Enterprise dla bezpiecznej pracy zdalnej

- Niezezwalanie i niezachęcanie do korzystania z urządzeń osobistych (PC) do profesjonalnej wymiany danych i komunikacji
- Zapewnienie pracownikom prywatnego i bezpiecznego dostępu
- Automatyzacja aktualizacji oprogramowania w całej sieci przedsiębiorstwa
- Zwracanie uwagi na podejrzane zapytania e-mailowe
- Używanie certyfikowanego oprogramowania. Audyty i certyfikaty zapewniają uwierzytelnianie zabezpieczeń oprogramowania.
- Uproszczenie procesów decyzyjnych. W sytuacjach awaryjnych dyrektor ds. bezpieczeństwa informacji lub dyrektor ds. informatyki muszą szybko podejmować decyzje w celu rozwiązania problemów, aby zapewnić ciągłość usług.

Broszura

Zadbaj o bezpieczeństwo swojej firmy, gdy wymagana jest praca zdalna



Sześć zaleceń ALE dotyczących bezpiecznej łączności zdalnej



1. Automatyczne przypomnienia o zmianie hasła

Pomoc pracownikom w zmianie korporacyjnych haseł przed ich wygaśnięciem. Przed wygaśnięciem hasła pracownicy codziennie otrzymają wiadomość e-mail z instrukcjami z prośbą o zmianę hasła.

2. Umożliwienie tworzenia kopii zapasowych danych w chmurze

Umożliwienie i zachęcanie pracowników do regularnego zapisywania danych w celu uniknięcia strat w przypadku problemów z laptopami. Udostępnienie miejsca do przechowywania kopii zapasowych danych i oferowanie zdalnej pomocy poprzez obsługę informatyczną lub specjalistów działu IT w razie potrzeby.

3. Przypominanie pracownikom o najlepszych praktykach w zakresie ochrony urządzeń

Utrzymywanie laptopa w jak najlepszym stanie:

- Wyłączanie laptopa na koniec każdego dnia (unikanie trybu uśpienia/zablokowania)
- Utrzymywanie laptopów z dala od źródeł ciepła (takich jak słońce lub grzejnik)
- Unikanie spożywania posiłków i picia przy laptopach
- Zabezpieczenie kabli przed dziećmi i zwierzętami domowymi

4. Bezpieczeństwo przede wszystkim

Szkolenie zespołów na temat zagrożeń i najlepszych praktyk bezpieczeństwa

- Zachęcanie pracowników do zastanowienia się przed kliknięciem na linki w mailach, nawet jeśli wyglądają one na wysłane przez kogoś znajomego.
- Zaoferowanie działań następczych w zakresie IT w przypadku wątpliwości

- Udostępnianie narzędzi do zgłaszania podejrzanych wiadomości e-mail
- Wykorzystanie grywalizacji do stworzenia kultury, która stawia na bezpieczeństwo: w ALE wykorzystaliśmy grywalizację, aby zachęcić pracowników do wykrywania i zgłaszania podejrzanych wiadomości e-mail

5. Komunikacja

Izolacja sprawia, że ludzie są narażeni na ataki cybernetyczne. Znajdź sposoby na utrzymanie łączności między swoimi zespołami:

- Organizuj regularne aktualizacje, wirtualne spotkania, wydarzenia, przestrzenie do współpracy, happy hour
- Zachęcaj ludzi do regularnego łączenia się ze swoimi zespołami
- Regularnie wysyłaj wiadomości e-mail, aby poinformować pracowników, że zespół IT jest dostępny, aby pomóc i przypomnieć im o najlepszych praktykach w zakresie bezpieczeństwa.

6. Zachęcanie do wprowadzania zdrowych nawyków związanych z łącznością

Ryzyko związane z pracą zdalną to 12-godzinny dzień pracy z ciągłą łącznością lub napiętym grafikiem wirtualnych spotkań. Zachęcaj pracowników do spędzania czasu z dala od komputera i rozłączania się oraz do spędzania czasu z rodziną lub na świeżym powietrzu.



Alcatel-Lucent Rainbow™ do współpracy w sieci

Rainbow: platforma do współpracy w chmurze, prowadzenia rozmów na czacie, rozmów audio i wideo, a także do udostępniania ekranu i dokumentów zapewnia pracownikom ALE narzędzi potrzebnych do pozostania w kontakcie. W okresie #WFH platforma ta jest szeroko wykorzystywana przez wszystkich pracowników do współpracy z kolegami.

Ponadto nasi partnerzy i klienci również przyjęli Rainbow jako preferowane rozwiązanie do współpracy. Platforma Rainbow spełnia wymagania bezpieczeństwa sektora publicznego, obrony narodowej, opieki zdrowotnej i innych konkretnych sektorów i jest zgodna z rygorystycznymi normami bezpieczeństwa, w tym między innymi: RODO, ISO 27001, HDS.



Rainbow™



Broszura

Zadbaj o bezpieczeństwo swojej firmy, gdy wymagana jest praca zdalna



Wspieranie społeczności

W ramach kampanii Business Continuity firma Alcatel-Lucent Enterprise zaoferowała setki tysięcy bezpłatnych licencji w celu wsparcia przedsiębiorstw, miast i rządów, aby pomóc im w utrzymaniu ciągłości usług. Ponadto, aby sprostać rosnącemu zapotrzebowaniu, a także zwiększające się liczbie użytkowników, rozszerzyliśmy nasze możliwości hostingu w chmurze.

Więcej najlepszych praktyk w zakresie cyberbezpieczeństwa można znaleźć w zaleceniach Europejskiej Agencji ds. Cyberbezpieczeństwa.

www.al-enterprise.com Nazwa i logo Alcatel-Lucent są znakami towarowymi firmy Nokia używanymi przez ALE na podstawie uzyskanej licencji. Inne znaki handlowe używane przez spółki zależne ALE Holding można znaleźć na stronie www.al-enterprise.com/en/legal/trademarks-copyright. Wszystkie inne znaki handlowe należą do odpowiednich właścicieli. Zawarte w tym dokumencie informacje mogą ulec zmianie bez uprzedzenia. ALE Holding ani żadna z jej spółek zależnych nie ponoszą odpowiedzialności za jakiegokolwiek nieścisłości zawarte w tym dokumencie. © 2023 ALE International. Wszelkie prawa zastrzeżone. DID20060201PL (Mar 2023)