



Udržujte své podnikání v bezpečí, když je vyžadována práce na dálku

Sebastian Roche, ředitel bezpečnosti informací společnosti Alcatel-Lucent Enterprise, sdílí pohledy na přístup společnosti ALE ke kontinuitě a bezpečnosti podnikání v této komplexní době

Nová realita #WFH

S nedávnou mezinárodní zdravotní krizí a celosvětově zavedenými opatřeními pro pobyt doma jsou společnosti, které dříve nenabízely možnost práce z domova (#WFH), nyní vyzývány k transformaci svých organizací, aby zajistily kontinuitu a bezpečnost podnikání.

V roce 2008 zahájila společnost Alcatel-Lucent Enterprise strategii práce z domova, kterou přijalo více než 50 % z 2 000 zaměstnanců pracujících v 50 kancelářích po celém světě. S více než polovinou zaměstnanců ALE pracujících z domova jsme již měli síťovou a IT architekturu potřebnou pro podporu práce na dálku. Výzvou byla fakticky otázka, jak bychom přešli z 50 % online pracovníků na 100 %.

Připraveno k akci

Ve třech letech před nedávnou zdravotní krizí, se společnost ALE pustila do rozsáhlé transformace IT. Byla přijata síťová architektura WAN definovaná službou, která poskytovala cloudové zabezpečení k proaktivnímu blokování vláken, k identifikaci potenciálních útoků a k zajištění bezpečného přístupu zaměstnanců.

Transformace zahrnovala:

- Zabezpečení v cloudu pomocí virtuálních přístupových bodů
- Trasování v reálném čase
- Identifikace neobvyklých vzorců chování pro detekci hrozeb





Příprava = Agilní reakce v krizových situacích

Rozhodnutí zahájit práci na dálku v pondělí bylo učiněno předchozí páteční odpoledne. Zaměstnanci dostali pokyn, aby si s sebou vzali své notebooky a monitory domů. V pondělí ráno začala práce jako obvykle, bez přerušení, když zaměstnanci začali svůj den ze svých vzdálených kanceláří. Dříve provedená transformace sítě zajišťovala bezpečné vzdálené připojení bez ohledu na to, kde se zaměstnanci nacházeli.

Výzva ohledně přístupu

Jednou z hlavních výzev, kterým jsme čelili, byly uživatelské profily, včetně týmů výzkumu a vývoje a technické podpory, které mají specifické potřeby pro přístup k určitým serverům a vývojovým platformám, což naše řešení vzdáleného přístupu neumožnilo. Tyto uživatelské profily zaměstnanců prošly jiným řešením soukromého přístupu než ostatní týmy.

Kdy začala snaha o přechod všech zaměstnanců na #WFH, přizpůsobili jsme naši infrastrukturu tak, abychom zvýšili naši šířku pásma a byli schopni podpořit nárůst počtu vzdálených připojení požadovaných zaměstnanci pracujícími z domova.

Klíčem je bezpečnost

Bezpečnost a ochrana podnikových dat jsou v nejistých dobách nesmírně důležité a ovlivňují mnoho organizací zpracovávajících citlivá data, jako jsou organizace veřejného sektoru, ministerstva, velká města a malá města.

Než jsme v ALE vůbec začali mluvit o #WFH, nasadili jsme distribuovanou a zabezpečenou infrastrukturu, stejně jako plně cloudové řešení privátního připojení pro všechny zaměstnance, abychom zajistili bezpečný vzdálený přístup k síti. Zachovali jsme existující řešení VPN (virtuální soukromé sítě) pro malé procento týmů, které měly specifické potřeby, například připojení IP telefonů ve svých vzdálených kancelářích. Zaměstnancům jsme také poskytli profesionální počítače se schopností spravovat automatické stahování a aktualizace softwaru.

Zavřete dveře před narušením bezpečnosti

Jak se dalo očekávat, během tohoto období rozsáhlé práce na dálku došlo k nárůstu hovorů a e-mailů týkajících se podezřelých e-mailů a žádostí o aktualizace hesel. Viděli jsme také prudký nárůst phishingových útoků a cílených útoků na zranitelný software.

Zatímco používání proxy chrání ALE před hlavními problémy s kybernetickou bezpečností, stále vidíme denně nová narušení pocházející z e-mailů, stahování nebo z neaktualizovaných verzí software/OS.

Udržujte komunikaci otevřenou

Během této náročné doby jsme udržovali nepřetržité virtuální spojení s týmy ALE. Pravidelně komunikujeme, sdílíme tipy a osvědčené postupy, a zajišťujeme, aby byl náš tým k dispozici pro podporu všech zaměstnanců.

Kontrolní seznam ALE pro bezpečnou práci na dálku

- Nedovolte ani nepovzbuzujte k používání osobních zařízení (PC) pro profesionální výměnu dat a komunikaci
- Zajištěte pro zaměstnance soukromý a zabezpečený přístup
- Automatizujte aktualizace softwaru v celé podnikové síti
- Věnujte pozornost podezřelým e-mailovým požadavkům
- Používejte certifikovaný software. Audity a certifikace zajišťují ověřování zabezpečení softwaru.
- Zjednodušte své rozhodovací procesy. V nouzových situacích musí CISO (ředitel bezpečnosti informací) nebo CIO (ředitel pro informace) rychle rozhodovat o řešení problémů, aby byla zajištěna kontinuita služeb

Brožura

Udržujte své podnikání v bezpečí, když je vyžadována práce na dálku



Šest doporučení ALE pro bezpečné vzdálené připojení



1. Automatizace připomenutí změny hesla

Pomozte zaměstnancům změnit firemní hesla dříve, než vyprší jejich platnost. Před vypršením platnosti obdrží zaměstnanci denní e-mail s pokyny, které je vyzývají ke změně hesla.

2. Umožněte zálohování dat v cloudu

Dovolte zaměstnancům a povzbuzujte je, aby pravidelně ukládali svá data, aby nedošlo ke ztrátě v případě problému s notebooky. Umožněte úložné prostory pro zálohování dat a podle potřeby poskytněte vzdálenou pomoc prostřednictvím IT Service Desk nebo IT specialistů.

3. Připomeňte zaměstnancům osvědčené postupy ochrany zařízení

Udržujte svůj notebook ve špičkovém stavu:

- Vypněte notebook na konci každého dne (vyhněte se režimu spánku/uzamčení)
- Udržujte notebooky mimo dosah zdrojů tepla (jako je slunce nebo topení)
- Vyvarujte se jídla nebo pití vedle notebooků
- Zabezpečte kabely před dětmi a domácími mazlíčky

4. Bezpečnost především

Vzdělávejte týmy ohledně rizik a osvědčených postupů v oblasti bezpečnosti

- Povzbudte zaměstnance, aby si dvakrát rozmysleli, než kliknou na odkazy v e-mailech, i když to vypadá, že je poslal někdo známý
- Nabídněte následná IT opatření v případě pochybností

- Poskytněte nástroje pro hlášení podezřelých e-mailů
- Použijte gamifikaci k vytvoření kultury bezpečnost především: V ALE, jsem použili gamifikaci, abychom povzbudili zaměstnance k detekci a hlášení podezřelých e-mailů

5. Komunikujte

Izolace činí lidi zranitelnými vůči kybernetickým útokům. Najděte způsoby, jak udržet své týmy ve spojení:

- Organizujte pravidelné aktualizace, virtuální schůzky, události, místa spolupráce, šťastnou hodinku
- Povzbuzujte lidi, aby se pravidelně spojili se svými týmy
- Posílejte pravidelné e-maily, aby zaměstnanci věděli, že IT tým je k dispozici, aby jim pravidelně pomáhal a připomínal osvědčené postupy v oblasti bezpečnosti

6. Podporujte zdravé návyky pro připojení

Riziko při práci na dálku je 12 hodinový pracovní den s nepřetržitým připojením nebo se schůzkami jedna za druhou. Povzbudte zaměstnance, aby měli čas odpojení a bez obrazovky a aby trávili čas s rodinou nebo venku.



Alcatel-Lucent Rainbow™ pro propojenou spolupráci

Rainbow: cloudová platforma spolupráce pro chat, videohovory a audio hovory, stejně jako pro sdílení obrazovky a dokumentů, jež poskytuje zaměstnancům ALE nástroje, které potřebují k tomu, aby zůstali ve spojení. Během této doby #WFH byla platforma široce využívána všemi zaměstnanci ke spolupráci s kolegy.

Kromě toho naši partneři a zákazníci také přijali Rainbow jako svou volbu řešení spolupráce. Rainbow řeší bezpečnostní požadavky veřejného sektoru, obrany, zdravotnictví a dalších specifických sektorů a je v souladu s přísnými bezpečnostními předpisy, mimo jiné: GDPR, ISO 27001, HDS.



Brožura

Udržujte své podnikání v bezpečí, když je vyžadována práce na dálku



Podpora naší komunity

Jako součást kampaně Kontinuita podnikání nabídla společnost ALE zdarma stovky tisíc licencí na podporu podniků, měst a vlád, aby jim pomohla udržovat kontinuitu služeb. Kromě toho, abychom řešili rostoucí poptávku stejně jako rostoucí počet uživatelů, jsme rozšířili naši kapacitu cloudového hostingu.

Další osvědčené postupy kybernetické bezpečnosti najdete v doporučeních agentury [EU pro kybernetickou bezpečnost](#).

www.al-enterprise.com Název a logo společnosti Alcatel-Lucent jsou ochranné známky společnosti Nokia používané v licenci ALE. Chcete-li zobrazit další ochranné známky používané přidruženými společnostmi společnosti ALE Holding, navštivte: www.al-enterprise.com/en/legal/trademarks-copyright. Všechny ostatní ochranné známky jsou majetkem příslušných vlastníků. Předložené informace mohou být změněny bez předchozího upozornění. Společnost ALE Holding ani její přidružené společnosti nepřebírají žádnou odpovědnost za nepřesnosti obsažené v tomto dokumentu.
© Copyright 2023 ALE International, ALE USA Inc. Všechna práva vyhrazena ve všech zemích. DID20060201CZ (Březen 2023)

