Trend Micro™

EMAIL SECURITY

Ndaloni më shumë sulme phishing, ransomware dhe mashtrime duke përdorur një përzierje teknikash kundër kërcënimeve

Kërcënimet e bazuara në email, përfshirë ransomware-t dhe kompromentimin e emailit të biznesit (BEC), po rriten në mënyrë eksponenciale dhe është e vështirë të mbahet i njejti ritëm. Edhe punonjësit tuaj më të zgjuar mund të klikojnë gabimisht në një URL me qëllim të keq dhe ta ekspozojnë ndërmarrjen tuaj ndaj krimit kibernetik.

TrendMicro™ Email Security ndalon më shumë sulme phishing, ransomware dhe BEC. Mundësuar nga XGen™, kjo siguri përdor një përzierje optimale të teknikave të kërcënimeve, si machine learning, analiza e sandbox, parandalimi i humbjes së të dhënave (DLP) dhe metoda të tjera për të ndaluar të gjitha llojet e kërcënimeve të shërbimeve email. TrendMicro™ Email Security mbron Microsoft® Exchange, Microsoft® Office 365®, Gmail™ dhe zgjidhje email të hostuara lokalisht.

FORRESTER®
WAVE LEADER 2021
Enterprise Email Security

BENEFITET KRYESORE

Mbrojtje e shtresëzuar: Siguron mbrojtje gjithëpërfshirëse për phishing, email-et spam duke përdorur teknika të shumta, që përfshirë dërguesin, analizën e përmbajtjes dhe figurës, inteligjencën artificiale dhe më shumë.

- **Mbrojtja nga mashtrimi me email**: Mbron kundër BEC me inteligjencë artificiale të përmirësuar dhe rregullat e ekspertëve për të analizuar titullin dhe përmbajtjen e emailit. Përfshin ADN-në e Stilit të Shkrimit TrendMicro si një shtresë shtesë për të kryer analiza autorësie për mbrojtjen BEC. (Licenca e Trend Micro™ Cloud App Security kërkohet për ADN-në e Stilit të Shkrimit).
- **Mbrojtja e shfrytëzimit të dokumentit**: Zbulon malware të avancuar që përdorin PDF, Microsoft® Office dhe dokumente të tjera duke përdorur logjikë statike dhe heuristike për të zbuluar dhe ekzaminuar anomalitë.
- **Mbrojtje e avancuar nga kërcënimet**: Zbulon malware të panjohur duke përdorur teknika pa model, siç është inteligjenca artificiale.
- **Nxjerrja e fjalëkalimit të skedarit**: Nxjerr ose hap skedarë të mbrojtur me fjalëkalim duke përdorur një kombinim të fjalëkalimeve të përcaktuara nga përdoruesit dhe përmbajtjes së mesazheve.
- **Koha e klikimit të URL-së**: Bllokon emailet me URL keqdashëse para mbërritjes dhe kontrollon përsëri sigurinë e URL-së kur një përdorues klikon mbi të.
- **Verifikimi dhe vërtetimi i burimit**: Përfshin Kornizën e Politikave të Dërguesit (SPF), Postën e Identifikuar të Çelësave të Domainit (DKIM), Autentifikimin e Mesazheve me bazë Domain, Raportimin dhe Përputhshmërinë (DMARC).
- **Inteligjenca e kërcënimit**: Përdor TrendMicro Network Smart Protection Network, e cila është një nga bazat e të dhënave më të mëdha të inteligjencës së kërcënimit për të lidhur Web-in, postën elektronike, skedarët, regjistrat e domeneve dhe shumë burime të tjera kërcënimi për të identifikuar infrastrukturën e sulmuesit para se të dërgohen.
- **Kriptimi i postës elektronike**: Kriptimi i postës elektronike i drejtuar nga politika të shkumta përfshin shërbimin e menaxhimit të çelësave dhe u mundëson marrësve të lexojnë email-e të koduar në çdo pajisje duke përdorur një shfletues Web-i.
- **DLP**: Përfshin modele DLP për ta bërë më të lehtë gjurmimin, dokumentimin dhe ruajtjen e informacionit konfidencial dhe të ndjeshëm.
- **Vazhdimësia e postës elektronike**: Siguron një sistem të postës elektronike në gatishmëri që jep përdorim të pandërprerë të postës elektronike në rast të ndërprerjes së serverit të email-it.
- **Raportim fleksibël**: Gjeneron raporte bazuar në përmbajtje të planifikuar dhe të personalizueshme.
- **Mbrojtja e kërcënimit të lidhur**: Sinkronizohet me TrendMicro Apex Central™ për të zbatuar një listë të objekteve të dyshimta të skedarëve dhe URL-ve.

ÇFARË TRENDMICRO EMAIL SECURITY MUND TË BËJË PËR TY:

Ndalon phishing dhe spam

- Shqyrton vërtetësinë dhe reputacionin e dërguesit të postës elektronike për të kontrolluar dërguesit me qëllim të keq
- Analizon përmbajtjen e postës elektronike duke përdorur një sërë teknikash për të filtruar spam dhe phishing
- Mbron nga URL-të me qëllim të keq në marrje dhe në kohën e klikimit (rishkruan dhe analizon URL-të në kohën e klikimit dhe i bllokon ato nëse janë me qëllim të keq)

Zbulon dhe bllokon kërcënimet e përparuara

- Zbulon dhe bllokon ransomware dhe lloje të tjera malware-sh duke përdorur inteligjencën artificiale, analizën makro dhe zbulimin e shfrytëzimit.
- Inteligjena Artificiale filtron malware të panjohur, duke rritur efikasitetin e mbrojtjes së avancuar të kërcënimeve
- Ndan informacione kërcënuese me shtresat e tjera të sigurisë për t'u mbrojtur nga sulmet e vazhdueshme dhe të synuara

Mbrojtje nga BEC

- Shqyrton sjelljen e postës elektronike (një ofrues i pasigurt i postës elektronike, domein i falsifikuar, ose një përgjigje për një shërbim falas të postës elektronike), qëllimin (implikimet financiare, urgjencën ose një thirrje për veprim) dhe autorësinë (stili i shkrimit)
- Ju lejon të keni fleksibilitetin për të përcaktuar listën e përdoruesve të profilit të lartë të organizatës tuaj për mbrojtjen BEC

Ju jep paqe mendore

- Përfshin mbështetje teknike 24/7
- Të gjitha email-et nga klientët në Evropë, Lindjen e Mesme dhe Afrikë (EMEA) dërgohen në qendrat e të dhënave në Evropën Perëndimore. Email-et nga Australia dhe Zelanda e Re dërgohen në qendrat e të dhënave në Australi. Email-et nga pjesa tjetër e botës dërgohen në qendrat e të dhënave në Shtetet e Bashkuara
- Shërbimi kryesor është i vendosur në qendrat e të dhënave AWS të certifikuara nga ISO 27001. Qendrat e të dhënave në rajone të ndryshme funksionojnë në mënyrë të pavarur dhe nuk janë të ndërlidhura për shkak të privatësisë së të dhënave dhe konsideratave sovrane

AFTËSITË E TREND MICRO EMAIL SECURITY

AFTËSIA	STANDART	AVANCUAR
Analiza dhe vërtetimi i dërguesit të postës elektronike nga SPF, DKIM dhe DMARC	Po	Po
Mbrojtje: Kërcënimet e njohura (spam, malware dhe URL me qëllim të keq)	Po	Po
Mbrojtje: Zbulimi i malware-ve të panjohur	Detektimi i Shfrytëzimit & Inteligjena Artificiale	Detektimi i Shfrytëzimit, Inteligjena Artificiale & Analiza Sandbox
Mbrojte: Mbrojtje e URL-ve të panjohura	Koha e klikimit të URL-së	Koha e klikimit të URL-së & Analiza URL Sandbox
Mbrojtje: Mashtrimi i bazuar në inteligjencën artificiale (AI)/zbulimi i BEC, kontrollimi i titullit të emailit dhe përmbajtjes	Po	Po
Mbrojtje: Mashtrimi i bazuar në AI/zbulimi i BEC, kontrollimi i autorësisë së dërguesit të postës elektronike	-	Po*
Nxjerrja e fjalëkalimit të skedarit	-	Po
Pajtueshmëria: DLP dhe kriptimi i postës elektronike	Po	Po
Raportimi: Raporte të personalizueshme dhe të planifikuara	Po	Po
Eksportim i regjistrave	Po	Po
Mbrojtja e kërcënimit të lidhur: Zbatimi i listave të objekteve të dyshimta të skedarëve dhe URL-ve nga Apex Central	Po	Po
Karantina e përdoruesit fundor	Po	Po
Vazhdimësia e postës elektronike: Siguron përdorim të pandërprerë të postës elektronike në rast të ndërprerjes së serverit të postës	-	Po
Dritarja e kërkimit të gjurmimit të postës	30 ditë	60 ditë

*Kërkohet licenca e Cloud App Security

vodafone business

Ju lutemi kontaktoni përfaqësuesin tuaj të shitjeve Vodafone për më shumë informacion

KËRKESAT E SISTEMIT

Për më shumë detaje dhe versionin e fundit të mbështetur vizitoni: Email Security

TREND MICRO™

Securing Your Connected World

[DS02_Trend_Micro_Email_Security_2107I9US]