TEGRA SYSTEMS

Tegra Verify

Når medarbejderen er i tvivl, får de svar på sekunder.



AI-baseret analyse af mistænkelige e-mails. Medarbejderen videresender mailen, og få sekunder senere har de en klar vurdering, en forståelig begrundelse og besked om, hvad de skal gøre. IT-afdelingen får overblikket.

~10 sek.
fra indrapportering til svar i indbakken

3 lag
automatiske kontroller, omdømme og AI

1 klik
for at indrapportere – intet at installere

Dansk udviklet og drevet · Svar og portal på dansk · tegra-systems.dk

Phishing rammer mennesker, ikke firewalls

De farligste mails kommer igennem spamfiltret: falske fakturaer, ændrede kontonumre, login-sider der ligner Microsoft 365, og mails der udgiver sig for at være direktøren. Medarbejderen er den sidste forsvarslinje – men står ofte alene med tvivlen.

Uden Tegra Verify

Mailen sendes til IT, som ikke når at svare før medarbejderen har handlet. Eller den bliver slettet uden at nogen lærer af den. Kollegerne får den samme mail i morgen.

Med Tegra Verify

Medarbejderen får en vurdering på sekunder og ved præcis hvad de skal gøre. IT ser alle indrapporteringer samlet, og systemet genkender kampagnen næste gang.

Sådan virker det

1

Videresend

Medarbejderen videresender den mistænkelige mail som vedhæftning – med ét klik på en knap i Outlook eller et andet mailprogram.

2

Analyse i lag

Automatiske kontroller af afsender, links og vedhæftninger. Omdømme fra tidligere sager. AI vurderer kun de mails, hvor der stadig er tvivl.

3

Svar på sekunder

Et tydeligt svar med vurdering, begrundelse og konkrete råd – og et link til hele analysen i kundeportalen.

Svaret medarbejderen får

TEGRA SYSTEMS

Vurdering af den indrapporterede mail

PHISHING

Sikkerhed: høj

BEGRUNDELSE

- Afsenderdomænet dinvirksornhed[.]dk efterligner jeres eget domæne dinvirksomhed.dk.
- Et link viser portal[.]dinvirksomhed[.]dk, men fører til en helt anden side.

HVAD SKAL DU GØRE

- Klik ikke på links, og slet mailen. Har du klikket, så kontakt IT med det samme.

Se hele analysen >

Analyse i lag – billigt først, AI sidst

Tegra Verify kombinerer hurtige, gennemsigtige kontroller med AI. Det gør vurderingen både præcis og forklarlig – og holder prisen pr. mail nede.

Afsender og autentificering

SPF, DKIM og DMARC. Domæner der efterligner jeres egne (fx dinvirksornhed.dk mod dinvirksomhed.dk, homoglyffer og punycode). Svaradresser der peger et andet sted hen.

Links og vedhæftninger

Links hvor den viste tekst ikke passer med destinationen, links direkte til IP-adresser og farlige filtyper som .exe, .html og dobbelte filendelser.

Beskyttede personer

Direktion og økonomi registreres med navn og kendte adresser. Mails der låner navnet eller efterligner adressen markeres – den klassiske direktørsvindel.

Omdømme og hukommelse

Afsendere, domæner, links og filer fra tidligere phishing genkendes på tværs af kunder. Kun indikatorer deles – aldrig mailindhold.

AI når der er tvivl

Kun de uklare mails vurderes af AI, som finder det reglerne ikke kan: påskud, hastværk, betalings- og loginanmodninger. Identiske mails genbruger svaret.

Mennesket har sidste ord

En gennemsigtig regelmotor træffer beslutningen, ikke AI'en. En menneskelig vurdering overskriver altid den automatiske – og huskes næste gang.

Sikkerhed og data er bygget ind fra start

- AI-motoren har ingen adgang til postkasser og kan ikke handle – den giver kun en vurdering.
- Mailindhold behandles som upålideligt og isoleres, så indlejrede instruktioner ikke kan styre analysen.
- Hver kunde ser kun egne data – håndhævet i selve databasen (row-level security).
- SPF, DKIM og DMARC på alle svar. Omkostning pr. kunde og pr. analyse logges fra dag ét.

Overblik for IT – og for medarbejderen

Kundeportalen giver alle et sted at følge med. Medarbejdere opretter sig selv med deres arbejdsmail, og administratoren styrer resten.

Medarbejder	Læseadgang	Administrator
Ser sine egne indrapporteringer med vurdering, begrundelse, råd og hvilke domæner mailen linker til.	Ser alle virksomhedens indrapporteringer – fx til IT-support eller en ekstern konsulent.	Retter vurderinger, inviterer kolleger og konsulenter, udpeger administratorer og styrer sikkerheden.

Konsulenter og partnere

Eksterne brugere markeres tydeligt og kan have adgang til flere kunder med ét login.

Selvbetjening med kontrol

Medarbejdere opretter sig med arbejdsmail og bekræfter via link. Oprettelse kan begrænses til virksomhedens IP-adresser – forsøg udefra logges.

Sikkerhedslog

Afviste oprettelser, invitationer og ændringer af roller og indstillinger logges med IP og browser.

Dashboard og statistik

Phishing, spam og legitime mails over tid, uafklarede sager og hvem der indrapporterer.

Kom i gang på en dag

1. Vi opretter jeres virksomhed og domæner og inviterer jeres administrator.
2. I tilføjer en knap i Outlook eller jeres mailprogram, der videresender mistænkelige mails som vedhæftning.
3. I tillader vores svaradresse i jeres mailsystem – fx Microsoft 365, Google Workspace eller Exchange – og så er I i gang.

Samarbejder med jeres phishing-træning

Bruger I MetaCompliance, KnowBe4, Hoxhunt eller lignende til phishing-træning? Tegra Verify genkender testmails fra træningssystemet og giver medarbejderen ros med det samme: "Godt gået – det var en øvelse, og du gjorde præcis det rigtige." Testkampagner holdes uden for statistik og omdømme, så billedet af de rigtige angreb ikke forstyrres. Genkendelsen sættes op pr. leverandør i kundeportalen.

Tegra Verify DMARC – beskyt jeres domæne

Phishing rammer ikke kun jeres medarbejdere. Kriminelle forfalsker også jeres domæne og sender mails i jeres navn til kunder og leverandører. DMARC er standarden, der stopper det – men den er svær at få rigtig uden overblik. Som tilkøb samler Tegra Verify rapporterne og viser jer, hvad I skal gøre.

Se, hvem der sender i jeres navn

Google, Microsoft og andre modtagere sender hver dag rapporter om al mail, der er sendt i jeres domænes navn. Tegra Verify samler dem og viser, hvilke servere der sender, og om de består SPF og DKIM.

Legitimt og forfalsket adskilt

Hver afsender, der ikke består, vurderes: godkendt (en rigtig afsender, fx et faktureringssystem, der skal rettes) eller forfalskning. Så ved I, hvad der er jeres, og hvad der ikke er.

Stram politikken trygt

Tegra Verify vejleder om, hvornår domænet er klar til at gå fra overvågning til karantæne og afvisning – først når de legitime afsendere består, og der er nok data. I bestemmer tempoet.

Test af opsætningen

En DNS-test tjekker DMARC, SPF, DKIM og MX for hvert domæne og viser præcis de DNS-poster, der skal oprettes eller rettes.

Jeres domæner i kundeportalen

Administratorer og læsebrugere ser status for hvert af virksomhedens domæner. Administratorer kan vurdere afsendere direkte i portalen.

Også til domæner, der ikke bruges

Holding-domæner uden mailtrafik beskyttes mod misbrug med afvisning og en SPF-post, der forbyder al afsendelse.

Sådan kommer I i gang

1. I opretter én DNS-post, der sender DMARC-rapporterne til Tegra. Vi tilknytter domænet i kundeportalen.
2. Efter et par uger har I overblikket: hvem der sender, hvad der består, og hvad der mangler at blive rettet.
3. I strammer politikken i jeres eget tempo, med vejledning fra portalen, til forfalskede mails afvises.

Rapporterne indeholder kun IP-adresser, antal og resultater – aldrig mailindhold – og slettes efter 13 måneder.

Nyt og på vej

Tegra Verify starter med indrapportering – men det er kun begyndelsen. Her er det nyeste, og hvad vi arbejder hen imod.

NYT

Tegra Verify Feed

Tilkøb: jeres firewall eller mail-gateway henter Tegras blokeringslister over phishing-IP'er, -domæner og -links automatisk – fx FortiGate. Mere på feed.tegra-systems.dk.

Tegra Verify DMARC

Tilkøb: overblik over, hvem der sender i jeres domænes navn, vurdering af afsendere og vejledning til at stramme politikken – også til holding-domæner. Status for hvert domæne i kundeportalen.

Kampagnegenkendelse

Mails med næsten samme indhold genkendes som én kampagne – også når navn og links varierer fra modtager til modtager.

Tegra Verify Watch (pilot)

Løbende kontrol af indgående mail via journalisering. Kun mistænkelige mails gemmes og vises for administratorer.

PÅ VEJ

Tidslinje for hver mail

Se præcis hvornår mailen kom ind, blev analyseret og besvaret – og hvem der rettede vurderingen.

Har andre også fået den?

Når én medarbejder indrapporterer, ser I med det samme, hvem ellers i virksomheden har modtaget samme kampagne.

PLANLAGT

Microsoft 365-integration

Microsofts Rapportér-knap direkte, sikkerhedsalarmer og indbakkeregler – kun med jeres samtykke.

Fjern fra alle indbakker

Når en kampagne er bekræftet, fjernes den fra alle modtageres postkasser med ét klik.

Vil I være med fra start?

Kontakt Tegra Systems for en demo og en snak om, hvordan Tegra Verify passer til jer.

tegra-systems.dk