De rol van AI in e-mailbeveiliging

Barracuda

De evolutie van e-mailfraude

E-mail vormt nog steeds het favoriete startpunt voor cybercriminelen om aan te vallen. Infiltratie van een organisatie kan op elk niveau plaatsvinden — phishing is niet alleen gericht op directieleden. Zodra aanvallers de inloggegevens van een persoon hebben, kunnen ze toegang krijgen. Als ze eenmaal in het netwerk zitten met één set inloggegevens, kunnen aanvallers zich gemakkelijker zijdelings verplaatsen en meer machtigingen en toegang krijgen. Zelfs toegang tot de mobiele telefoon van een werknemer kan leiden tot bredere netwerktoegang.

Vroeger waren frauduleuze e-mails vaak slecht geschreven en eerlijk gezegd ongelooflijk. Criminelen vertrouwden op een 'spray and pray'-aanpak: ze stuurden duizenden berichten uit in de hoop dat er een paar zouden werken. Traditionele gateway-verdedigingen zijn behoorlijk bedreven in het omgaan met deze grootschalige aanvallen. De voortdurende analyse van e-mails van klanten door Barracuda toont aan dat 16% van al het e-mailverkeer uit grootschalige aanvallen bestaat, zoals spam, malware en andere e-mails met een kwaadaardige payload. U hebt nog steeds gateway-verdedigingen nodig om deze aanvallen, die een reëel gevaar blijven, te stoppen.

Phishing, echter, speelt een heel ander spel. Barracuda beschouwt slechts 0,1% van de berichten als gepersonaliseerde phishing-aanvallen. Maar hoewel de cijfers niet hoog zijn, is het potentiële gevaar zeer reëel. Achter dit kleine aantal berichten gaan zeer vastberaden en doelgerichte criminelen schuil.

De phishing- en imitatie-e-mails van vandaag de dag lijken afkomstig te zijn van iemand die u kent en ze vragen u om te handelen op een manier die logisch en verstandig lijkt. Financiële afdelingen krijgen betalingsverzoeken van CEO's en CFO's. De berichten zijn afkomstig van wat lijkt op een echt adres. Er is een verklaring waarom betaling via een andere methode nodig is: een urgente kans voor het bedrijf, of de noodzaak om een genoemde en correcte leverancier te betalen om te profiteren van een speciale aanbieding. E-mails worden getimed voor het einde van de maand, wanneer financiële afdelingen het druk hebben en mogelijk minder alert zijn.

Criminelen zijn meesters in het snel imiteren van nieuwe berichtformaten. Waarschuwingen voor het vergrendelen van accounts zijn een steeds vaker voorkomende manier om een gebruiker te dwingen dringende maatregelen te nemen. Maar criminelen zetten ook pagina's op zakelijke services van derden, zoals Dropbox, OneDrive of Google Drive, op om inloggegevens te verzamelen. Deze zijn moeilijk te herkennen, aangezien bedrijven en hun klanten afhankelijk zijn van een steeds grotere verscheidenheid aan cloudservices voor samenwerking en het delen van bestanden. Deze berichten worden doorgaans niet opgepikt door gateway-beveiligingen, omdat de e-mails zelf geen schadelijke lading bevatten.

Waarom kunnen traditionele gateway-verdedigingen het niet aan?

De uitdaging van e-mailbeveiliging ligt in de schaalbaarheid en flexibiliteit ervan. De oude manieren om bekende domeinen te blokkeren werken niet meer, omdat gecompromitteerde domeinen zo snel veranderen. Omdat aanvallen geen gemakkelijk te detecteren payload bevatten, zijn ze erg moeilijk te blokkeren bij de gateway.

Regels instellen om berichten te markeren werkt niet als aanvallen zo snel veranderen.

De nadelen van het op deze wijze verdedigen van een gateway omvatten continu praktijkgericht beheer en een groot risico op fout-positieven en fout-negatieven. Aan zo'n systeem zijn ook infrastructuur- en computingkosten verbonden: elke toegevoegde regel betekent meer verwerkingstijd.

En naarmate het aantal aanvallen toeneemt, raken bestaande systemen — en het personeel — overweldigd.

Elk systeem dat afhankelijk is van regels loopt het risico op aanvallers met geautomatiseerde systemen die uw regels bijna net zo snel kunnen leren kennen als u ze implementeert. Dat betekent niet dat u geen gateway-beveiliging nodig hebt. Dergelijke verdedigingen zijn nog steeds uitstekend in het blokkeren van kwaadaardige payloads en spam, waar de meerderheid van slechte mails uit bestaat.

Goede e-mailbeveiliging door middel van AI kan de meeste aanvallen blokkeren en het aantal meldingen waarvoor menselijke tussenkomst vereist is, drastisch verminderen.

Hoe kan AI u beschermen tegen phishingaanvallen?

AI zet de kracht van data science en machine learning in om metagegevens, inhoud, context en typisch gebruikersgedrag te onderzoeken.

AI kan taken uitvoeren die normaal door mensen worden gedaan. Het kan de spelling van het domein en de kopteksten van e-mails controleren en verdachte e-mails beter filteren dan eenvoudige of op lijsten gebaseerde systemen.

Maar AI kan verder gaan dan traditionele verdedigingsmechanismen. AI gebruikt natuurlijke taalverwerking om naar de context en betekenis van de hele boodschap te kijken.

Goede AI leert uw organisatie en omgeving kennen om de beste verdediging te bieden door afwijkingen en ongebruikelijke communicatie op te sporen. Als AI meer inzicht krijgt in uw gebruikers, is het beter in staat om phishingpogingen te blokkeren en is de kans kleiner dat fout-positieven worden gesignaleerd.

Als iemand een ongebruikelijk verzoek indient, een ongebruikelijk e-mailadres gebruikt of iemand om een gunst vraagt aan een persoon die hij of zij nooit eerder heeft gesproken, kan AI dit abnormale gedrag snel signaleren. Het kan zelfs een verandering in toon in een bericht vaststellen — als een gebruiker beleefder of veeleisender wordt.

Phishing-e-mails hebben enkele kenmerken gemeen. Ze vragen vaak om snelle reacties, zodat mensen geen tijd hebben om na te denken. Ze eisen vaak geheimhouding, waardoor mensen worden ontmoedigd om contact op te nemen met anderen.

AI-systemen kunnen niet alleen grote hoeveelheden gegevens snel verwerken, maar hier zelfs beter van worden. Ze zijn in staat om sociale engineering-aanvallen op te sporen, terwijl standaardbeveiliging voor een e-mailgateway deze doorlaat. Het beheer van goed ingerichte AI-systemen is goedkoper, aangezien er minder menselijk toezicht of beheer nodig is dan bij traditionele e-mailbeveiliging. Ook kunnen AI-systemen in de cloud snel worden opgeschaald wanneer dat nodig is.

Effectieve methoden op het gebied van AI: de juiste provider kiezen

Het probleem bij het kiezen van een AI-beveiligingsprovider is dat u te maken hebt met een soort 'black box'. Het is dus belangrijk om u te concentreren op resultaten uit de echte wereld in plaats van te luisteren naar lijsten met schijnbare mogelijkheden die het systeem biedt.

Dat betekent dat we moeten kijken naar de effectiviteit van de detectie — hoe het systeem voor uw organisatie presteert. Barracuda en enkele andere leveranciers bieden manieren om de effectiviteit van deze systemen te testen. Er zijn geen kosten verbonden aan het gebruik van Email Threat Scanner van Barracuda in het Postvak IN van gebruikers om de kwaadaardige e-mails te vinden die uw huidige verdediging heeft gemist. Ongeveer 16.000 organisaties hebben de gratis scanner gebruikt en 12 miljoen bedreigingen in hun Postvak IN gevonden.

U moet ook vragen stellen over het percentage fout-positieven, het percentage fout-negatieven en hoe deze cijfers in de loop van de tijd veranderen naarmate systemen intelligenter worden.

Goede systemen kunnen eenvoudig worden geïntegreerd in uw bestaande beveiligingsinfrastructuur en vereisen niet veel of geen investeringen in de infrastructuur. Ze moeten ook flexibiliteit bieden in de manier waarop ze aanvallen bestrijden en hoe ze gegevens verstrekken voor rapportage en andere analysetools. En natuurlijk moet AI het leven van beveiligingsteams makkelijker maken, in plaats van nog meer ruis en onnodige alarmen en waarschuwingen toe te voegen.

Bezoek onze website voor meer informatie over e-mailbeveiliging met AI van Barracuda.

Over Barracuda

Bij Barracuda willen we van de wereld een veiligere plek maken. Wij zijn van mening dat ieder bedrijf toegang verdient tot een cloud-first beveiligingsoplossing op bedrijfsniveau die makkelijk aan te schaffen, te implementeren en gebruiken is. Wij beschermen e-mails, netwerken, gegevens en applicaties met innovatieve oplossingen die meegroeien en zich aanpassen aan het traject van onze klant. Meer dan 200.000 organisaties over de hele wereld vertrouwen op Barracuda om hen veilig te houden, zelfs wanneer ze niet eens weten dat iets een risico vormt, zodat zij zich kun richten op hun bedrijf. Ga voor meer informatie naar barracuda.com.

Barracuda