Grip op e-mailbeveiliging

Hét handboek om grip te krijgen op de beveiliging van e-mail

MITE3

Grip op e-mailbeveiliging

Hét handboek om grip te krijgen op de beveiliging van e-mail

Joram Teusink

Colofon

Titel: Grip op e-mailbeveiliging
Auteur: Joram Teusink
Uitgever en druk: Brave New Books

E-mail: publishing@mite3.nl

Plaats van uitgave: Nederland
Jaar van uitgave: 2024
Eerste druk: 2024
ISBN: 978-94-650-1933-8

Vormgeving en opmaak: Joram Teusink, met lettertypes Roboto Slab en Roboto Mono
Informatieve illustraties: Ontworpen door Joram Teusink
Artistieke illustraties: Gegenereerd met LLM-technologie DALL-E via ChatGPT
Omslag: Ontwerp door Joram Teusink, foto via Shutterstock

Inhoudsopgave

Colofon **3**
Inhoudsopgave **4**
Introductie tot E-mail Security **11**
Het belang van E-mail Security 11
De rol van e-mail in moderne communicatie 12
Belang van e-mailbeveiliging 13
Gevolgen van aanvallen via e-mail 14
Historische context en evolutie van e-mail bedreigingen en maatregelen 15
Van ARPANET tot phishing 16
De dynamiek van aanvallers en verdedigers 17
Innovaties in de beveiliging van e-mail 18
Geavanceerde e-mail dreigingen **21**
Phishing, Spear-Phishing en Whaling aanvallen 21
Inleiding tot phishing 22
Verschillen tussen phishing, spear-phishing en whaling 22
Technieken en tactieken van phishers 24
Case-studie: Diefstal van € 19 miljoen bij Pathé 25
Inleiding 26
Achtergrond 26
Analyse van de case 26
Reactie van de organisatie 27
Conclusie 27
BEC (Business E-mail Compromise) aanvallen 28
Inleiding tot het overnemen van e-mailaccounts 29
Meest voorkomende doelen 30
Potentiële schade voor organisaties 30
Case-studie: De diefstal van 118.000 euro bij Haarlemmermeer 31
Inleiding 32
Achtergrond 32
Analyse van de case 32
Reactie van de organisatie 33
Conclusie 33
Ransomware via e-mail 34
Inleiding tot ransomware aanvallen via e-mail 35
De weg van ransomware via e-mailbijlagen en kwaadaardige links 36
Financiële, operationele en reputatieschade door ransomware 37
Case-studie: De ransomware aanval bij de Universiteit Maastricht 38
Inleiding 39

Achtergrond ... 39
Analyse van de case ... 39
Reactie van de organisatie ... 40
Conclusie ... 42
Basisprincipes van e-mail ... 43
Hoe het verzenden en ontvangen van e-mail werkt ... 43
Verzenden van e-mail met SMTP ... 44
Ontvangen van e-mail met POP3 ... 44
Synchroniseren van e-mail met IMAP ... 45
Versleuteling van SMTP, POP3 en IMAP ... 46
Synchronisatie van het e-mail account met CalDAV en CardDAV ... 46
Synchroniseren met iCalendar ... 47
E-mail headers en hun betekenis ... 48
De functie van e-mailheaders ... 49
Inzichten in een beveiligingsonderzoek ... 49
De basis headers van e-mail ... 50
Headers voor het organiseren van e-mail threads ... 52
Headers voor e-mail authenticiteit en integriteit ... 53
Privacyoverwegingen bij e-mailheaders ... 54
Manipulatie van headers en detectiemethoden ... 55
De dynamiek van beveiligingsmaatregelen ... 56
Introductie ... 56
De dynamiek van de maatregelen ... 57
De volgorde van de maatregelen ... 58
Autonome beveiligingsmaatregelen ... 59
Introductie ... 60
Overzicht van maatregelen ... 60
Interactieve beveiligingsmaatregelen ... 61
Introductie ... 62
Overzicht van maatregelen ... 62
E-mail filtering ... 66
Microsoft 365 ... 66
Overzicht van beveiligingsfuncties in Microsoft 365 ... 67
Configuratie en best practices ... 68
Google Workspace ... 70
Overzicht van beveiligingsfuncties in Google Workspace ... 71
Configuratie en best practices ... 72
Email Security Gateways ... 73
Introductie ... 74
Functies van Email Security Gateways ... 74
Noodzaak voor Email Security Gateways ... 76
E-mailversleuteling ... 77
Het versleutelen van het transport ... 77

Het belang van e-mailtransportversleuteling ... 78
Het proces van e-mailtransportversleuteling ... 79
Normen van e-mailtransportversleuteling ... 81
Implementeren van e-mailtransportversleuteling ... 82
Overweging bij e-mailtransportversleuteling ... 83
Het versleutelen van het bericht ... 84
Het belang van e-mailberichtversleuteling ... 85
Het proces van e-mailberichtversleuteling ... 86
Normen van e-mailberichtversleuteling ... 88
Implementeren van e-mailbericht versleuteling ... 89
Het verliezen van de sleutel ... 90
Alternatieven voor S/MIME en OpenPGP ... 91
Centrale opslag en beveiliging ... 91
Voordelen van deze aanpak ... 93
Nadelen van deze aanpak ... 93
Beleid voor transportversleuteling met MTA-STS ... 94
Wat is MTA-STS en het doel ervan ... 95
Configuratie en implementatie ... 96
Implementatie op hoofdlijnen ... 96
Opbouw van een MTA-STS-beleid op de webserver ... 97
Voorbeelden van MTA-STS-beleid ... 99
Hosten van het MTA-STS-beleid ... 100
Opbouw van een MTA-STS-beleid in de DNS ... 101
Per domein een aparte configuratie ... 101
Valideren van het MTA-STS-beleid ... 102
Typische problemen en oplossingen met MTA-STS ... 103
Onvolledige of ontbrekende DNS-configuratie ... 103
Verlopen of ongeldige certificaten ... 103
Missende e-mailservers in het MTA-STS-beleid ... 104
Gewijzigd beleid wordt niet herkend ... 104
Monitoren van transportversleuteling met TLS-RPT ... 105
Wat is TLS-RPT en het belang ervan ... 106
Configuratie en implementatie ... 106
Implementatie op hoofdlijnen ... 106
Opbouw van een TLS-RPT-beleid ... 107
Per domein een aparte configuratie ... 108
Valideren van een TLS-RPT-beleid ... 108
Typische problemen en oplossingen met TLS-RPT ... 109
Geen DNS-record, geen rapportage ... 109
Verifiëren van TLS-certificaten met DANE ... 110
Wat is DANE en waarom het belangrijk is ... 111
Configuratie en implementatie van DANE ... 112
Aanpak bij eigen e-mailservers ... 112

Aanpak bij e-mailservers derde partijen....113
Typische problemen en oplossingen met DANE....115
Afhankelijkheid van DNSSEC....115
Aanpassingen in de DNS-configuratie en certificaatbeheer....115
Geen universele ondersteuning....116
Meer administratie en foutgevoeligheid in processen....116
E-mailauthenticatie....117
Preventie van spoofing van e-mail met SPF....117
Wat is SPF en waarom het belangrijk is....118
Hoe SPF werkt....119
Het opzetten en configureren van SPF-records....119
Mechanismen in een SPF-record....119
Modifiers in een SPF-record....121
Macro's in een SPF-record....124
Gebruik van macro's....125
Enkele voorbeelden van SPF-records....126
Per domein een aparte configuratie....127
Valideren van een SPF-record....127
Het proces van SPF-validatie....128
Typische problemen en oplossingen met SPF....131
Meer dan 10 DNS lookups in een SPF-record....131
Overschrijding van DNS record grootte....134
Onvolledige SPF-records....135
Fouten in de syntaxis van SPF-records....135
Overmatig vertrouwen op het SPF mechanisme....136
Dubbele SPF-records in de DNS aanwezig....137
Gebruik van de oude type SPF-records....137
Integriteitsborging van e-mail met DKIM....138
Wat is DKIM en waarom het belangrijk is....139
Hoe DKIM werkt....140
Het opzetten en configureren van DKIM-records....140
Tags in een DKIM-record....140
Een voorbeeld van DKIM-record via TXT....142
DKIM-records in een CNAME-record....142
Een voorbeeld van een DKIM-record via CNAME....142
Digitale handtekeningen en sleutels....143
Per domein een aparte configuratie....144
Valideren van een DKIM-record....144
Het proces van DKIM-validatie....145
Typische problemen en oplossingen met DKIM....147
Ongeldige handtekeningen in e-mail....147
Dubbele handtekeningen in e-mail....148
Dubbele selectors in de DNS....148

Verlopen sleutels in de DNS....148
Compatibiliteitsproblemen met clients....149
Beheer van private sleutels....149
Overschrijding van DNS record grootte....149
Handhaving en rapportage met DMARC....150
Wat is DMARC en waarom het belangrijk is....151
Hoe DMARC werkt....152
Het opzetten en configureren van DMARC-records....152
Tags in een DMARC-record....152
Enkele voorbeelden van DMARC-records....154
Beleidsopties in DMARC....155
Rapportageopties in DMARC....156
Identifier alignment in DMARC....157
Configuratie per hoofddomein of subdomein....158
Valideren van een DMARC-record....159
Het proces van DMARC-validatie....161
Rapportage en analyse van DMARC gegevens....164
Typische problemen en oplossingen met DMARC....166
Te strikte DMARC-beleid....166
Onjuiste DMARC-configuratie....167
Interactie met andere beveiligingsprotocollen....167
Verwerken van DMARC-rapporten....167
Merkidentiteit verstevigen in e-mail met BIMI....168
Wat is BIMI en waarom het belangrijk is....169
Hoe BIMI werkt....170
Het opzetten en configureren van BIMI-records....170
Tags in een BIMI-record....170
Enkele voorbeelden van BIMI-records....171
Logo in SVG Tiny formaat....171
Het gebruik van een Verified Mark Certificate (VMC)....172
Per domein een aparte configuratie....173
Valideren van een BIMI-record....174
Typische problemen en oplossingen met BIMI....175
Risico's van niet-authentieke logo's....175
Configuratiefouten in BIMI-records....175
Ontbreken van een adequaat DMARC-beleid....175
Beperkte ondersteuning door e-maildiensten....176
BIMI zonder het gebruik van een VMC....176
Domeinen niet gebruikt voor e-mail....177
Het belang van het beschermen van alle domeinen....178
Bescherming met SPF, DKIM en DMARC....179
Valkuilen bij het beschermen van niet-e-mail domeinen....180
Geparkeerd domein wordt misbruikt voor spam en phishing....180

Over het hoofd zien van subdomeinen ... 180
Verlopen van domeinregistraties ... 181
Risico van DNS-spoofing en poisoning ... 181
Bulk e-mail etiquette ... 182
Juist versturen van bulk e-mail ... 182
Wat is bulk e-mail en waarom is het anders? ... 183
Definitie van bulk e-mail ... 183
Verschil tussen transactionele en bulk e-mails ... 183
Doelen en gebruiksscenario's ... 183
De uitdagingen van schaalgrootte ... 183
Het belang van lijsthygiëne en het beheren van opt-ins/opt-outs ... 184
Definitie van lijsthygiëne ... 184
Voordelen van een schone lijst ... 184
Opt-in/opt-out procedures ... 184
Het beheren van inactieve abonnees ... 184
Het belang van feedback loops en het omgaan met bounces ... 185
Wat zijn Feedback Loops ... 185
Reageren op klachten ... 185
Soorten bounces ... 185
Automatisering van Bounce Management ... 185
IP-warming en opbouwen van verzendreputatie ... 186
Wat is IP-warming ... 186
Waarom IP-warming nodig is ... 186
Stappen voor effectieve IP-warming ... 186
Het monitoren van de IP-reputatie ... 187
Technologie bij bulk e-mail ... 187
De Unsubscribe header ... 187
Links voor afmelden of abonnement wijzigen ... 188
Implementatie van e-mailbeveiliging technologieën ... 189
Het monitoren van de e-mail deliverability ... 190
Wat is deliverability ... 190
Factoren die deliverability beïnvloeden ... 190
Spamfilters en hun criteria ... 190
Feedback en aanpassing ... 190
Valkuilen bij bulk e-mail verzending ... 191
Oververzending ... 191
Niet naleven van wet- en regelgeving ... 191
Niet naleven van de etiquette ... 191
Lijsten van slechte kwaliteit ... 191
Niet reageren op feedback ... 191
Praktische gids voor het invoeren van e-mailbeveiliging ... 192
Een blauwdruk voor implementatie ... 192
Introductie ... 193

Stap 1: Voorbereiding....193
Stap 2: Instellen e-mailbeveiliging inkomende e-mail....196
Stap 3: Invoeren van basis e-mailauthenticatie....196
Stap 4: Versterken van e-mailauthenticatie....198
Stap 6: Toepassen van bulk e-mail etiquette....200
Essentiële vragen voor uw ICT en e-maildienstverleners....201
Introductie....202
Vragenlijst....202
Nawoord....204
Appendix A: Woordenlijst....205
Appendix B: Overzicht e-mailtools....215
Over de auteur....217

Introductie tot E-mail Security

Het belang van E-mail Security

De rol van e-mail in moderne communicatie

Altijd nog een essentiële rol voor e-mail

In het huidige digitale tijdperk, waar diverse communicatiekanalen beschikbaar zijn, blijft e-mail een essentiële rol spelen in zowel persoonlijke als professionele communicatie. Het voortdurende gebruik van e-mail kan worden toegeschreven aan verscheidene factoren, die in de volgende paragrafen nader worden toegelicht.

Universele toegankelijkheid

E-mail is toegankelijk voor iedereen met een internetverbinding, ongeacht het apparaat of de locatie. Het unieke aspect van e-mail is dat het een van de weinige digitale communicatiemethoden is waarmee een bericht, inclusief bijlagen, van zowel een bekende als een onbekende afzender naar de inbox van een ontvanger kan worden verzonden, zonder autorisatie vooraf. Deze eigenschap is zowel een kracht als een kwetsbaarheid van e-mail.

Zakelijke communicatie normen

In het bedrijfsleven, ondanks de opkomst van zakelijke chatapps, vormt het ontbreken van integratie tussen verschillende chatapps een belemmering. E-mail is onafhankelijk van providers en wordt daarom vaak verkozen als het primaire communicatiemiddel in professionele contexten. Bovendien biedt e-mail de mogelijkheid tot het aangaan van juridisch bindende zakelijke overeenkomsten, een optie die ontbreekt bij chatapps.

Veelzijdigheid en archivering

E-mail biedt de mogelijkheid tot systematische archivering, waardoor het eenvoudig is om vroegere conversaties en uitgewisselde documenten terug te vinden. Deze functionaliteit is essentieel voor zakelijke en juridische doeleinden. Daarnaast ondersteunt e-mail het toevoegen van diverse bestandstypen aan berichten, waardoor het een flexibel medium is dat aan uiteenlopende communicatiebehoeften voldoet.

E-mail als universele identificatiemiddel

Een aspect van de relevantie van e-mail is het gebruik van het e-mailadres als gebruikersnaam bij tal van online diensten en platforms. Van sociale media, bankdiensten tot online winkelen, een e-mailadres is vaak vereist voor het aanmaken van een account en het inloggen. Hierdoor is het e-mailadres niet enkel een middel voor communicatie, maar ook een sleutel tot een groot deel van onze digitale levens.

Belang van e-mailbeveiliging

Beschermen van vertrouwelijkheid en privacy

Het beveiligen van e-mail is van essentieel belang om te voorkomen dat onbevoegden toegang krijgen tot e-mailberichten. Deze veiligheidsmaatregelen zijn bedoeld om de vertrouwelijkheid van uitgewisselde informatie te waarborgen en de privacy van zowel verzender als ontvanger te beschermen.

Bescherming voor verzender en ontvanger

Een goede e-mailbeveiliging kan zowel de verzender als de ontvanger beschermen. Het correct toepassen van beveiligingsprincipes voor e-mail zorgt niet alleen voor een veiligere uitwisseling van berichten, maar verhoogt ook de betrouwbaarheid van de bezorging. Dit is belangrijk voor e-mail die van commercieel belang zijn of die bijvoorbeeld gevoelige gegevens bevatten.

Voorkomen van cyberdreigingen

Beveiligingsmaatregelen voor e-mail zijn belangrijk om te verdedigen tegen schadelijke software zoals virussen, phishing en spoofing. Deze dreigingen kunnen de integriteit van e-mailcommunicatie ondermijnen en de reputatie van betrokkenen schaden.

Risico's van cyberaanvallen

E-mail is vaak het doelwit van cybercriminelen omdat het een centraal communicatiemiddel is in zowel het persoonlijke als professionele domein. Een beveiligingsincident kan leiden tot economische verliezen, reputatieschade en kan zelfs juridische gevolgen hebben.

De rol van e-mail in cyberaanvallen

Onderzoek wijst uit dat meer dan 90% van de cyberaanvallen begint met e-mails[1]. Deze kunnen variëren van frauduleuze activiteiten en phishing tot ransomware-aanvallen, het verspreiden van malware, social engineering en identiteitsdiefstal. Het opstellen van een doeltreffende aanpak voor e-mailbeveiliging is daarom cruciaal om deze bedreigingen het hoofd te bieden.

Implementatie van e-mailbeveiliging

Het opzetten van een goede aanpak voor e-mailbeveiliging moet een hoge prioriteit hebben binnen de strategie van een organisatie. Dit betreft niet alleen het afweren van externe bedreigingen, maar ook het garanderen van de authenticiteit en integriteit van digitale communicatie via e-mail.

[1] Security Management, 90 procent van de bedrijfsaanvallen begint met een phishing-e-mail: https://mite3.link/90-procent

Gevolgen van aanvallen via e-mail

Risico's voor individuen en organisaties

Wanneer de beveiliging van e-mail wordt geschonden, staan zowel individuen als organisaties bloot aan aanzienlijke risico's. Individuen kunnen geconfronteerd worden met het lekken van persoonlijke gegevens, inclusief financiële of medische informatie, wat het gevaar op identiteitsdiefstal en andere cybercriminaliteit doet toenemen.

Voor organisaties houdt een schending in dat vertrouwelijke informatie, zoals bedrijfsgeheimen, klantgegevens en interne berichtgeving, openbaar gemaakt kan worden. Dit kan financiële schade veroorzaken, het vertrouwen van klanten en zakenrelaties ondermijnen, en de reputatie schaden.

Juridische gevolgen

Het niet naleven van wet- en regelgeving, waaronder de AVG en CAN-SPAM, kan resulteren in aanzienlijke boetes. Dit benadrukt het belang en de noodzaak om persoonsgegevens te beschermen volgens de geldende wet- en regelgeving.

Kettingreactie van aanvallen

Een beveiligingslek kan de deur openen voor verdere aanvallen via het e-mailverkeer. Deze kunnen impact hebben op de oorspronkelijke getroffen partij, maar ook hun klanten, medewerkers en zelfs leveranciers en partners. Denk hierbij aan dat de aanvaller schadelijke e-mails als spam, phishing en pogingen tot fraude verstuurt via de e-mailsystemen van de getroffen partij.

Financiële verliezen

Aanvallen via e-mail kunnen directe financiële schade veroorzaken, van het betalen van losgeld bij ransomware-aanvallen tot verliezen door geslaagde phishingoperaties. Bijkomende kosten voor het herstel van systemen, beveiligingsadvies en juridische ondersteuning kunnen de financiële impact vergroten.

Reputatieschade

De reputatie van een organisatie kan ernstig lijden onder succesvolle aanvallen, wat kan resulteren in klantenverlies, omzetdaling en verminderde winstgevendheid. Voor beursgenoteerde ondernemingen kan dit zelfs leiden tot een afname van de aandelenwaarde.

Operationele disruptie

Aanvallen kunnen de operationele processen van een organisatie verstoren, met gevolgen voor kritieke systemen en processen. Dit kan toegang tot belangrijke informatie hinderen en de dagelijkse werkzaamheden van medewerkers belemmeren, wat leidt tot inefficiëntie en vertragingen.

Historische context en evolutie van e-mail bedreigingen en maatregelen

Van ARPANET tot phishing

De oorsprong van e-mail

De geschiedenis van e-mail neemt ons mee naar de vroege dagen van het internet. In de jaren 60 legde ARPANET (Advanced Research Projects Agency Network), de voorloper van het hedendaagse internet, de basis voor de eerste elektronische berichten[2]. Deze berichten, voornamelijk tekst zonder opmaak, markeerden het begin van digitale communicatie dat tegenwoordig het internet en het World Wide Web wordt genoemd.

De eerste e-mail en het @-teken

Ray Tomlinson verzond in 1971 het eerste e-mailbericht tussen twee computers en introduceerde het @-teken om de gebruiker van het domein te scheiden[3]. Deze conventie is nog steeds de norm.

Het idee dat zijn uitvinding zou leiden tot meer dan 300 miljard dagelijkse e-mails wereldwijd, gebruikt door meer dan 4,4 miljard mensen, zou Tomlinson vast hebben verbaasd.

Opkomst van cyberdreigingen

Naarmate e-mail populairder werd in de jaren 80 en 90, kwamen de eerste veiligheidsuitdagingen aan het licht. E-mail was in eerste instantie niet ontworpen met beveiliging als prioriteit, wat het een doelwit maakte voor cyberdreigingen zoals spam en de eerste e-mailvirussen.

Privacy en encryptie

De privacy van e-mailcommunicatie werd ook een zorg, gezien het gemak waarmee berichten onderschept konden worden. Dit leidde tot de ontwikkeling van encryptietools, zoals PGP (Pretty Good Privacy) en later STARTTLS voor versleuteld e-mailtransport, om de communicatie te beschermen.

Het eerste spambericht

Voordat het fenomeen 'spam' zijn naam kreeg, te danken aan een Monty Python sketch, werden gebruikers al overstelpt met ongewenste commerciële berichten. Het eerste bekende geval dateert uit 1978, gericht aan een grote groep ARPANET-gebruikers.

[2] NordVPN, What is ARPANET? The creation of the internet: https://mite3.link/what-is-arpanet
[3] Guinness World Records, 1971: First Ever Email: https://mite3.link/first-ever-email

Virussen verspreid via e-mail

Een van de eerste beruchte e-mailvirussen was het "ILOVEYOU"-virus in 2000, dat zich snel verspreidde door zichzelf automatisch naar contactpersonen te verzenden en bestanden te verwijderen[4]. Dit virus bereikte naar schatting 45 miljoen gebruikers en veroorzaakte meer dan 10 miljard dollar aan schade.

Phishingaanvallen

Phishing, het versturen van bedrieglijke e-mail die afkomstig lijkt uit betrouwbare bronnen om gevoelige informatie te stelen, begon in de jaren 90. Aanvallers richtten zich toen vooral op AOL-gebruikers door zich voor te doen als medewerkers van het bedrijf AOL[5].

De dynamiek van aanvallers en verdedigers

Kat-en-muisspel

In de wereld van digitale beveiliging vindt een constant spel plaats tussen cybercriminelen en beveiligingsexperts. Met de voortdurende vooruitgang in technologie ontdekken aanvallers nieuwe manieren om beveiligingsmaatregelen te omzeilen. Recentelijk richten ze zich steeds meer op het uitbuiten van menselijke kwetsbaarheden via methoden zoals social engineering, in plaats van enkel technische aanvalspunten.

Geëvolueerde phishing-technieken

De aanpak van phishingaanvallen is verschoven van brede, algemene campagnes naar meer gerichte aanvallen, zoals spear-phishing en whaling.

- **Spear-Phishing**: Hierbij verzamelen aanvallers specifieke informatie over hun doelwit om de betrouwbaarheid van hun frauduleuze berichten te verhogen. Deze informatie kan variëren van professionele connecties tot persoonlijke interesses.

- **Whaling**: Deze methode focust op hoge functionarissen binnen organisaties, zoals CEO's en directeuren, met als doel toegang te krijgen tot financiële middelen of gevoelige informatie. Whaling-aanvallen vereisen grondig onderzoek naar het doelwit voor maximale effectiviteit.

Deze technieken laten zien hoe cybercriminelen de mens, als ‘zwakste’ schakel, als hun voornaamste doelwit zien.

[4] CNN, ‘I love you‘: How a badly-coded computer virus caused billions in damage and exposed vulnerabilities which remain 20 years on: https://mite3.link/iloveyou-virus
[5] Phishing.org, History of Phishing: https://mite3.link/history-of-phishing

Ransomware via e-mail

Phishing is een populaire methode voor het verspreiden van ransomware via e-mail. Deze e-mails verleiden de ontvanger om kwaadaardige bijlagen te openen of op links te klikken die leiden tot de installatie van ransomware. Deze software versleutelt vervolgens bestanden en eist losgeld voor de ontsleuteling.

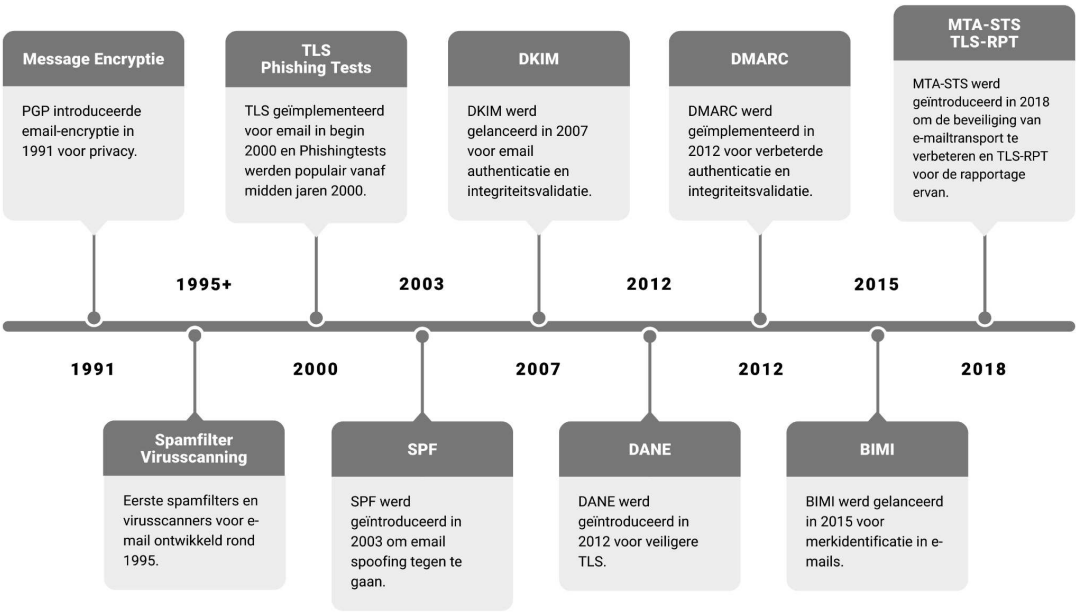
De kracht van deze aanvallen ligt in het manipuleren van emoties zoals nieuwsgierigheid en angst, met e-mail die lijken te komen van betrouwbare bronnen.

Wedstrijd zonder einde

In een landschap van digitale beveiliging ontwikkelen aanvallers voortdurend nieuwe methoden om door beveiligingslagen heen te breken. Ze richten zich steeds vaker op individuen met gerichte phishing-technieken en creëren geavanceerde malware om beveiligingssystemen te omzeilen. Het gebruik van e-mail als een aanvalsvector voor het verspreiden van phishing en ransomware laat het belang zien voor het invoeren van geavanceerde beveiligingsmaatregelen om deze dreigingen het hoofd te bieden.

Innovaties in de beveiliging van e-mail

Hieronder volgt een beknopt overzicht van de belangrijkste technologieën op volgorde van hun introductie op de markt.



E-mailversleuteling sinds 1991

End-to-end versleuteling (encryptie) zorgt ervoor dat alleen de verzender en beoogde ontvanger de inhoud van een e-mail kunnen lezen. Door het bericht te coderen met een unieke sleutel bij verzending, blijft de inhoud onleesbaar voor anderen, zelfs bij onderschepping. Hoewel deze techniek essentieel is voor het waarborgen van privacy, is universele adoptie nog geen realiteit.

Spamfilters geïntroduceerd in de late jaren '90

Met de groei van spam ontstonden initieel eenvoudige spamfilters, die evolueerden naar complexe systemen gebruikmakend van machine learning en gedragsanalyse. Initiatieven zoals "DNS-based Blackhole Lists" en "Spam URI Real-time Blocklists" helpen informatie over bekende spammers te delen. Hier werd niet alleen de gebruikerservaring verbeterd, maar ook de veiligheid nam toe.

Virusdetectie in e-mail vanaf de jaren '90

De opkomst van systemen voor e-mailbeveiliging gericht op het scannen van virussen markeerde een belangrijke stap voorwaarts. Moderne systemen gebruiken geavanceerde methoden zoals heuristische analyse om zelfs nog onbekende malware te identificeren, en waken over bijlagen en links in e-mail voor schadelijke inhoud.

Transportversleuteling begin jaren 2000

Versleuteling met TLS biedt een essentiële beveiligingslaag voor e-mail tijdens het transport over het internet, door de gegevens tussen servers te versleutelen. TLS zorgt ervoor dat, zelfs als gegevens worden onderschept, de inhoud onleesbaar blijft voor derden.

Phishing Awareness trainingen sinds midden jaren 2000

Het trainen van eindgebruikers in het herkennen van phishingaanvallen is één van de belangrijkste onderwerpen geworden om organisaties te beschermen. Simulaties van phishing-e-mails testen de waakzaamheid van medewerkers en kunnen de beveiligingscultuur binnen organisaties helpen te versterken.

Zichtbaarheid in e-mail domein spoofing sinds 2003

Anti-spoofing maatregelen zoals SPF helpen te bepalen welke mailservers geautoriseerd zijn om e-mail voor een domein te versturen. Dit vermindert de kans op succesvolle spoofing- en phishingaanvallen.

Waarborgen van integriteit van e-mail sinds 2007

DKIM voegt een digitale handtekening toe aan e-mailheaders. Dit helpt de ontvanger van het bericht te authenticeren om vast te stellen of het bericht onderweg niet is aangepast. Dit verzekert ontvangers van de authenticiteit van de e-mail.

Verbeterde e-mailauthenticatie en rapportage sinds 2012

DMARC biedt een beleid voor de behandeling van e-mail die niet aan SPF of DKIM voldoen en maakt "alignment" verificatie mogelijk. Dit versterkt de bescherming tegen spoofing van domeinnamen. Daarbij draagt DMARC bij aan het creëren van inzicht in het e-mailverkeer vanuit de organisatie op het vlak van SPF, DKIM en DMARC.

Certificaatpublicatie met DANE sinds 2012

DANE, een protocol dat DNSSEC gebruikt om TLS-informatie te publiceren, verhoogt de betrouwbaarheid van online diensten. Dit systeem adresseert de kwetsbaarheden van het CA-systeem door organisaties in staat te stellen TLS-certificaatinformatie direct in hun DNS-records te publiceren. Zo wordt de authenticiteit van de verbindingen versterkt door een extra verificatielaag toe te voegen, waardoor e-mail- en webverkeer veiliger wordt.

Merkbescherming met BIMI sinds 2015

BIMI biedt een innovatieve aanpak voor het valideren van de authenticiteit van e-mailafzenders. Door logo's in de inbox van de ontvanger weer te geven, maakt BIMI het gemakkelijker om legitieme e-mail te identificeren. Deze visuele indicator van authenticiteit verhoogt de herkenbaarheid en het vertrouwen in de communicatie van bekende merken. Voor het toepassen van BIMI moeten organisaties voldoen aan strenge e-mailauthenticatienormen, waardoor het een betrouwbare indicator is van legitieme correspondentie.

Versterking van e-mailtransport via MTA-STS sinds 2018

MTA-STS vermindert het risico op afluisterpraktijken door te verzekeren dat e-mail via versleutelde TLS-verbindingen wordt verzonden. Dit protocol maakt het mogelijk voor organisaties om beleid te publiceren dat strenge TLS-vereisten dicteert, waarmee de veiligheid tijdens e-mailtransport aanzienlijk wordt verbeterd.

Inzicht in transportversleuteling met TLS-RPT sinds 2018

TLS-RPT biedt organisaties waardevolle inzichten in de beveiliging van e-mailtransport door automatische rapportage over TLS-verbindingen. Dit protocol helpt bij het tijdig identificeren en oplossen van beveiligingskwesties, zoals configuratiefouten of pogingen tot Man-in-the-Middle-aanvallen, en draagt bij aan een veiliger e-mailverkeer.

Geavanceerde e-mail dreigingen

Phishing, Spear-Phishing en Whaling aanvallen