ddimail - der automatische E-Mail-Beantworter

+ automatische Verschlüsselung + integrierte Sicherheitsfunktionen + sicherer B2B-Geschäftsdatenaustausch + regelbasierte Weiterverarbeitung/Prozessautomatisierung

Nutzen Sie ***ddimail*** gegen die Flut von E-Mails mit gefährlichen Anhängen und verführerischen Inhalten und Links.
Verhindern Sie, dass Ihre persönlichen und vertraulichen (Geschäfts-)Daten ungeschützt auf den Mailservern weltweit Diebstahl und Manipulationen ausgesetzt sind.
Erfahren Sie mehr über die 6 größten Defizite und Gefahren klassischer E-Mails - und wie ***ddimail*** sie eliminiert und dabei viele Arbeitsschritte für Sie automatisiert.

1. **für jederman erreichbare Postfächer ermöglichen Angreifern die massenhafte automatisierte Zusendung pot. gefährlicher E-Mails**

Problem	jedermann kann E-Mails an jedes Postfach senden, aus bot-Netzen können Hacker ganz einfach tausende E-Mails versenden, die bei den Empfängern massiven manuellen Aufwand nach sich ziehen
bisherige Lösungsansätze	Die Identifikationen "menschlicher Absender" durch captures sind für den Nutzer extrem umständlich und nervig, es gibt Systeme, die fordern die Absender auf, die E-Mail zu ändern, bis sie deren Sicherheits-Spezifikationen entspricht, ohne mitzuteilen, welche das sind und andere Systeme senden noch während des E-Mail-Eingangs nach extrem schneller Prüfung eine NDR zurück, was den Absender an der Existenz der Adresse zweifeln lässt und pot. Neugeschäfte wohl regelmäßig verhindern dürfte
ddimail-Umsetzung	ddimail beantwortet eingehende E-Mails automatisch durch die Rücksendung einer Verifizierungsanforderung zur Bestätigung der Korrektheit des Absenders der E-Mail, Spam-E-Mails laufen ins Leere
Vorteile	ddimail reduziert den Aufwand und damit die Kosten für die Bearbeitung des massenhaften unseriösen Missbrauchs des eigenen E-Mail-Accounts, eine einmalig erforderliche Bestätigung verursacht dagegen nur minimalen Mehraufwand

2. **alle E-Mails gelangen auf Abruf mehr oder weniger gut gefiltert direkt in die IT-Systeme der tw. unbedarften Anwender**

Problem	durch den Abruf des eigenen E-Mail-Postfaches gelangen auch potentiell gefährliche E-Mails direkt auf die Arbeitsplatzrechner der Nutzer und werden erst danach durch die obligatorische Endpoint-Security-Software geprüft. Klassische Spam-&Malware-Filter haben jedoch immer gewisse Fehlerraten, sodass immer ein Restrisiko besteht, dass unerkannter Malware die PCs der Endempfänger erreicht, sowie andererseits legitime E-Mails Ihre Empfänger nicht erreichen. Daher bleibt die individuelle Prüfung jeder E-Mail und auch die Kontrolle der Quarantäne-Ordner obligatorisch. Durch gezielte Angriffe mittels social-engineering erhöht sich die Fehlerquote nochmals erheblich.
bisherige Lösungsansätze	E-Mail-Security-Lösungen, insb. sog. Secure-E-Mail-Gatways (SEG), bieten viele Funktionen zur Unterscheidung zwischen gewünschten und unerwünschten E-Mails, aber selbst ausgefeilte Technologien, wie Sandboxing oder die Nutzung von KI bieten keinen vollständigen Schutz vor unbekannten Risiken (ZERO-Day-Angriffen) oder aufwendig recherchierten, individuellen Angriffen auf Ihr Unternehmen.
ddimail-Umsetzung	ddimail ist ein dem E-Mail-Empfang vorgeschaltetes System, dass die E-Mail in seine Bestandteile zerlegt, gefährliche Elemente entschärft und nur sichere Komponenten für die weitere Bearbeitung zur Verfügung stellt, mit der CLIENT-SERVER-Version erfolgt dies auf einer separaten vorgelagerten VM, idealerweise unter Linux
Vorteile	ddimail trennt den risikobehafteten E-Mail-Empfang und die Verarbeitung der sicheren Inhalte in den lokalen IT-Systemen, mit der CLIENT-SERVER-Version können die Ports für den E-Mail-Empfang als risikoreiche Einfallstore für Hackerangriffe aller Art, geschlossen werden

3. **Spam-, Malware- und Phishing-Mails**

Problem: nervige Spams, gefährliche Malware und verführerische Phishing-Mails sind sowohl für Security-Software, als auch für Anwender immer schwerer erkennbar, insb. bei gezielten social-engineering-Angriffen auf Ihr Unternehmen

bisherige Lösungsansätze: Spam- und Malware-Filter mit Verschiebung in Quarantäneordner propagieren ein falsches Sicherheitsgefühlt, positiv- und negativ getestete E-Mails müssen trotzdem individuell auf Gefahren oder gegen möglichen Datenverlust geprüft werden, Mitarbeiter sind entsprechend zu schulen und zu sensibilisieren

ddimail-Umsetzung: mit ddimail verfolgen wir einen völlig anderen Ansatz, die E-Mail-Nutzung wirklich sicher zu machen:

- gegen Spam: anstatt einer fehlerbehafteten Sortierung in "gut" und "böse" nutzt ddimail eine eindeutige Absenderidentifikation durch Verifikation und ggf. Verschlüsselung sowie weitere Funktionen, wie Blacklisting von TLDs usw.
- gegen Malware: anstatt Endpoint-Security mit Blockade der Ausführung nutzt ddimail die obligatorische Antivirensoftware in einem vorgeschalteten System, idealwerweise ausgelagert in einer "VM" unter Linux, sowie div. Sicherheitsfunktionen gemäß der "Secure-E-Mail-Architecture (SEA)" von ddimail, wie die Entschärfung von ausführbaren Dateianhängen und Bereitstellung zum expliziten Nachladen u.v.m.
- gegen Phishing/gefährliche Inhalte und Links: anstatt Sensibilisierung aller Mitarbeiter bietet ddimail die Prüfung und Freischaltung der E-Mails und -Absender durch qualifizierte IT-Mitarbeiter in einem vorgelagerten System, sowie weitere Funktionen, wie die Umleitung von Links mit Hinweisen auf pot. Gefahren.

Vorteile: mit dem ddi-eMail-Client erhält der E-Mail-Empfänger ein einfaches Tool, über das er nur Zugriff auf seine vorab geprüften E-Mails erhält, damit entfällt der größte Risikofaktor - der vor dem Monitor. Und allzu erfinderischen Mitarbeitern kann mit "ddimail CLIENT/SERVER" auch der direkte Zugriff auf andere POP- und IMAP-Konten gesperrt werden

4. **E-Mails liegen auf den Mailservern unverschlüsselt vor**

Problem: der konsequente Verzicht auf eine Ende-zu-Ende-Verschlüsselung bei der Übertragung der E-Mails über die Server im Internet macht Datendiebstahl und -Manipulationn, wie z.B. der Bankverbindungen in Rechnungen zu einem so erfolgreichen Geschäftsmodell

bisherige Lösungsansätze: die Abstimmung einer Ende-zu-Ende-Verschlüsselung (E2EE) erwies sich bisher als zu umständlich und unpraktikabel, weswegen meistens darauf verzichtet wurde. Der Aufwand zur Nutzung aktuellster Sicherheitstechnologien ist zumindestens gem. eines Urteils des OLG Schleswig jedoch jedem Unternehmen zumutbar

ddimail-Umsetzung: ddimail bietet die automatische Abstimmung einer E2EE durch Angabe des eigenen PGP-Keys in der Verifikations-E-Mail, in den lokalen E-Mail-Clients stehen die Daten jedoch unverschlüsselt zur Verfügung

Vorteile: Das Urteil xyz des OLG Schleswig vom xx.x.xx macht deutlich, dass eine E2EE die praktisch alternativlose Technologie für die Übertragung insb. von persönlichen Daten gem. DSGVO und elektronischen Rechnungen ist. Auch gegen Proteste von Datenschützern ist der Einsatz auch kleineren Unternehmen zumutbar, um Schadensersatzansprüche wie in dem hier verhandelten Verfahren zu verhindern.

5. **Versender von E-Mails können die Absenderadresse frei wählen und damit leicht manipulieren**

Problem: die automatisierte "Dunkel"-Verarbeitung eingehender E-Mails ist aufgrund der nicht gewährleisteten korrekten Identifikation des Absenders von E-Mails praktisch nicht möglich

bisherige Lösungsansätze: einige E-Mail-Provider verhindern den Versand von E-Mails mit einer fremden Domain, die Provider der Spammer aber leider nicht, eine automatisierte E-Mail-Verarbeitung mit der Sicherheit von ddimail ist uns nicht bekannt

ddimail-Umsetzung: ddimail bietet sichere E-Mails durch eindeutige Identifikation des Absender anhand der Kombination der E-Mail-Adresse mit der "echten" Absenderkennung, erhöhte Sicherheit durch die Verschlüsselung mittels PGP-Key-Identifikation, bis hin zu maximaler Sicherheit

	mit "ddimail DIRECT" durch Nutzung des im EDI-Bereich etablierten AS2-Protokolls
Vorteile	sicherer B2B-Geschäftsdatenaustausch wie im EDI-Bereich üblich - jetzt auch per E-Mail.

6. **die Sicherheit der Zustellung von E-Mails kann nicht gewährleistet werden, E-Mails können unterwegs verloren gehen oder beim Empfänger unerkannt im Spam-Filter landen, ohne Rückmeldung an den Absender**

Problem	das SMTP-Protokoll beinhaltet keine obligatorische Empfangsbestätigung (MDN), die für rechssicheren und nachvollziehbaren Geschäftsdatenaustausch unerlässlich ist
bisherige Lösungsansätze	E-Mail-Clients bieten die manuelle Möglichkeit, MDNs anzufordern bzw. MDNs zu senden, allerdings nur unverbindlich, für rechtssicher nachvollziehbare Datenübermittlung nutzt man im EDI-Bereich das AS2-Protokoll
ddimail-Umsetzung	ddimail kann MDNs automatisch senden, mit ddimail wird "die Postkarte des Internets" zu einem Einschreiben mit Rückschein
Vorteile	Eine Bestätigung der Zustellung ist insb. für E-Rechnungen, aber auch für alle anderen kaufmännischen Dokumente, wie termingebundene Bestellungen, von elementarer Bedeutung, was der Versand per E-Mail bisher nicht gewährleisten konnte. Bieten Sie Ihren Geschäftspartnern die Rücksendung von MDNs und fordern Sie sie von Ihnen ein! Wenn diese das wegen des manuellen Aufwandes nicht garantieren können, verweisen Sie gerne auf ddimail.