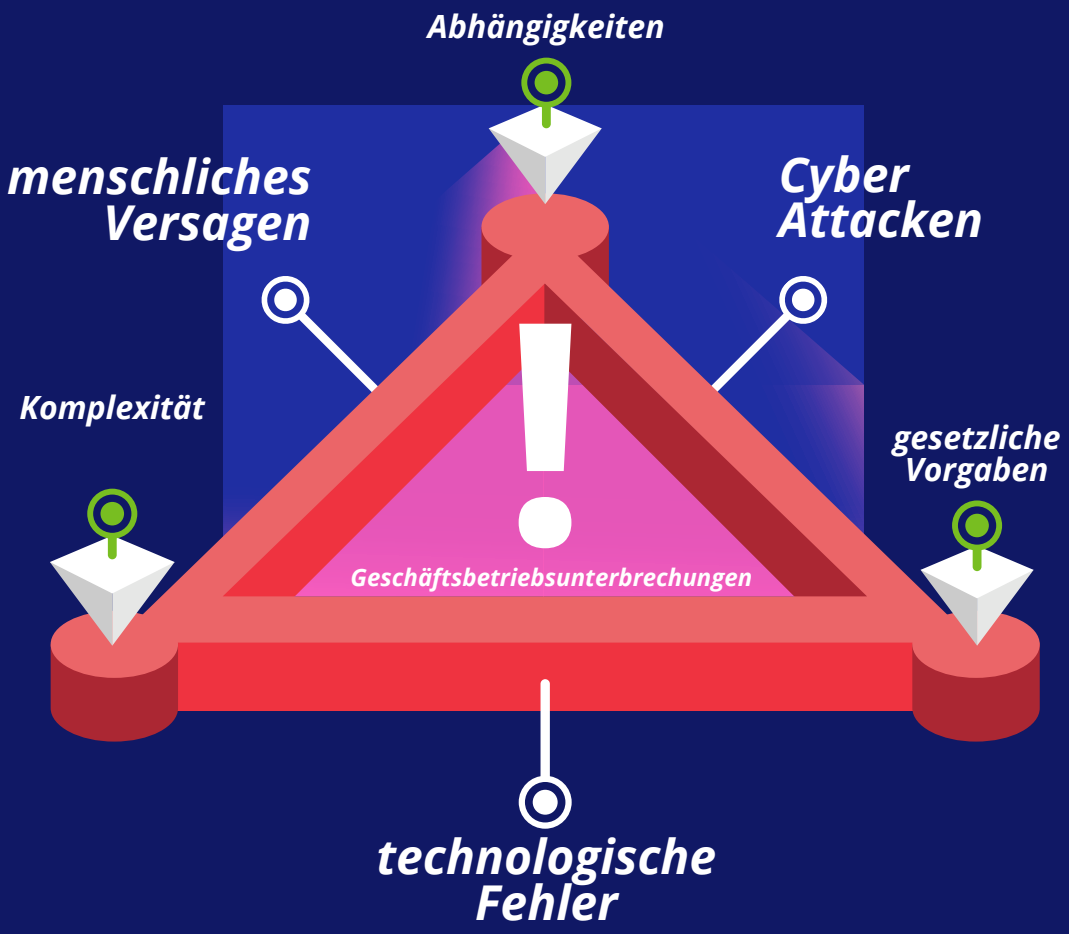
mimecast™

E-Mail Security 3.0

Eine umfassende E-Mail Security Sicherheitsstrategie

Welche Rolle Geschäftsunterbrechungen spielen

Führungskräfte und Geschäftsführer sind besorgt und planen für eine aktive Vorbeugung von Geschäftsbetriebsunterbrechungen. Selbst mit den ausgeklügeltsten Schutzvorkehrungen ist es unmöglich, vollständig vorherzusagen, woher Cyber Angriffe und Störungen kommen werden. Technologie ist nicht unfehlbar, Menschen machen Fehler, und (Cyber) Kriminelle werden nie aufhören nach neuen Möglichkeiten und Chancen zu suchen. Die damit verbundenen Risiken wachsen im Kontext der digitalen Welt exponentiell an. Eine irreversible Abhängigkeit von der Technologie und tief verwobene Lieferketten führen zu einem echten "Störungsdomino-Effekt", während die wachsenden regulatorischen Anforderungen die Komplexität noch weiter erhöhen.



Unterbrechungen verhindern

Fast alle Cyber-Angriffe nutzen E-Mail. Warum? Der E-Mail Verkehr hört niemals auf, E-Mails sind vertrauenswürdig, sie enthalten Links und Anhänge und können zudem leicht gefälscht werden. Früher bedeutete der Schutz vor E-Mail basierten Angriffen der Schutz des Perimeters, aber die Zeiten, in denen das reichte, sind lange vorbei. Unternehmen müssen jetzt von einem auf dem Perimeter basierenden Sicherheitsansatz zu einem allgegenwärtigen, umfassenden Ansatz übergehen.

Am Perimeter
(Ihrer Unternehmensgrenze)

- Komplexe und fokussierte Angriffe
- Gefahr sensible Daten zu verlieren

Innerhalb Ihres Netzwerks und Ihrer Organisation

- Gefahren ausgehend von internen E-Mails
- Gefahr menschlicher Fehler

Ausserhalb des Perimeters
(Ausserhalb Ihres Unternehmens)

- Missbrauch eigener Domains
- Markenimitationen

Am Perimeter - An Ihrer Unternehmensgrenze

Zone 1

Angreifer senden SPAM und Viren über E-Mails oder binden schadhafte URLs darin ein, um Phishing und Spear-Phishing-Angriffe durchzuführen. Sie liefern auch Formen von Malware, die Organisationen mit Signaturen und klassischen Antivirus-Technologien nicht erkennen können. Obwohl sich das traditionelle Konzept des “Perimeters” weiterentwickelt hat, bleibt die Tatsache bestehen, dass die Sicherung von E-Mails einer der wichtigsten Schritte für Unternehmen ist, um Risiken zu reduzieren und Störungen zu vermeiden.

Real-World Scenario

Paul’s Firma war kürzlich zu Office 365 migriert, so dass er nicht überrascht war, als er eine E-Mail sah, in der er aufgefordert wurde, seinen Benutzernamen und sein Passwort zu aktualisieren. Paul hat die Aktualisierung sofort vorgenommen. Ein paar Wochen später erhielt er eine E-Mail, in der es hieß, dass seine Dateien verschlüsselt worden waren und er eine Zahlung von 50.000 Dollar für die Freischaltung leisten solle. Er war Opfer einer Phishingattacke geworden und Angreifer hatten seine Zugangsdaten erbeutet. Da Paul in der Finanzabteilung arbeitete und Zugang zu sensiblen Daten hatte, bezahlte seine Firma.
Die Technologie von Mimecast hätte diesen Angriff verhindern können, indem sie jeden Klick in Echtzeit scannt und alle URLs in eingehenden E-Mails überprüft und neu schreibt.

Zone 1 - Herausforderungen
Phishing und Spear Phishing
Impersonation Attacken
Schadhafte URLs und Anhänge
Beeinträchtigungen des E-Mail Verkehrs

Innerhalb Ihres Netzwerks und Ihrer Organisation

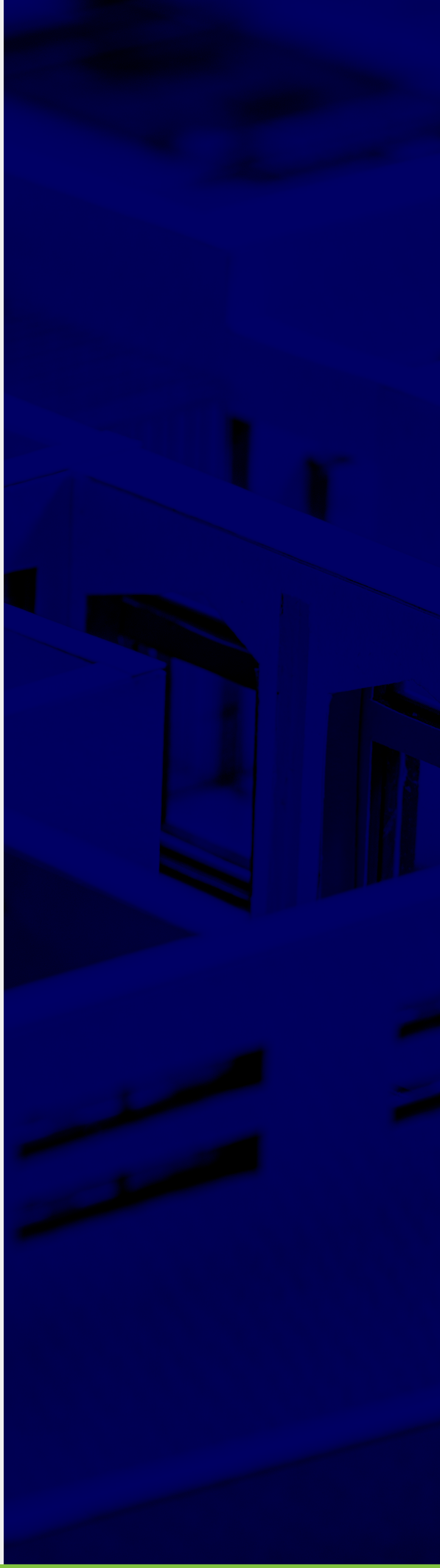
Zone 2

Selbst mit einem robusten E-Mail-Sicherheits-Perimeter können Angreifer die Abwehr umgehen und innerhalb eines E-Mail-Netzwerks operieren, indem sie kompromittierte Nutzerkonten oder Social Engineering nutzen, um schadhafte E-Mails an Mitarbeiter sowie Kunden und Partner zu versenden. Mitarbeiter sind auch anfällig dafür, dass sie Anhänge öffnen, auf Links klicken und damit auf Betrugsversuche hereinfallen. Es ist deshalb nicht überraschend, dass menschliches Versagen ein Faktor für den Großteil erfolgreicher Angriffe ist.

Real-World Scenario

Ein Freund von Maria schickte seinen Lebenslauf an ihre persönliche E-Mail-Adresse. Um ihm zu helfen, lud Maria den CV per Dropbox herunter, speicherte ihn auf ihrem Arbeitscomputer und leitete ihn ebenfalls an die Personalabteilung weiter. Als ihr Kollege die Datei öffnete, wurde schadhafter Code freigeschaltet, der in das Netzwerk der Organisation eindrang. Bevor die IT-Abteilung das Problem lösen konnte, waren E-Mails und Dateien von mehreren Mitgliedern des Führungsteams gelöscht worden. Da kein Archivierungssystem vorhanden war, konnten die Informationen nicht wiederhergestellt werden. Mimecast hätte diesen Angriff verhindern können, indem umfassende Inspektionen auch auf interne E-Mails angewandt werden und Awareness-Schulungen helfen, das Risiko menschlicher Fehler zu reduzieren.

Zone 2 - Herausforderungen
Attacken, die sich von Mitarbeiter zu Mitarbeiter ausbreiten
Attacken, die von Mitarbeitern auf Kunden und Partner übertragen werden
Menschliche Fehler / Fehlende Awareness
Dauerhaft verlorene Daten



Ausserhalb des Perimeters

Zone 3

Ohne sich sich überhaupt mit den gesicherten Unternehmensschnittstellen auseinandersetzen zu müssen, ist es für Angreifer recht einfach, sich im Internet als eine bestimmte Marke auszugeben. Selbst unbedachte Angreifer können eine ähnliche Markendomäne registrieren oder eine Website hosten, die dazu bestimmt ist, Kunden, Partner und Mitarbeiter zu täuschen, und so den Wert und das Vertrauen zerstören, welches Markeninhaber möglicherweise erst nach Jahren oder Jahrzehnten aufgebaut haben.

Real-World Scenario

Eine Universität in Australien wurde von Hackern angegriffen, welche die Universität-Website klonten, Phishing-E-Mails an Studenten geschickt und mit dem Sammeln ihrer Anmeldedaten begonnen haben. Der Angriff wurde zunächst nicht von der Universität, sondern von Mimecast entdeckt, da wir das Web kontinuierlich nach genau solchen Szenarien durchsuchen. Nachdem die Universität benachrichtigt wurde, nahm Mimecast die gefälschte Website in weniger als einer Stunde vom Netz. Und drei Tage später, als eine weitere gefälschte Website erschien, sah Mimecast sie und nahm sie ebenfalls direkt vom Netz, bevor weitere Studenten dem Betrug zum Opfer fallen konnten.

Zone 3 - Herausforderungen
Gefälschte E-Mails über Ihre Domains versendet
Markenimitationen
Gefälschte Webseiten
Ähnlich aussehende Domains

Die gesamte Security-Systemlandschaft

Komplexe Sicherheitsherausforderungen führen oft zu komplexen Systemlandschaften - eine Realität, die sich in der Tatsache widerspiegelt, dass Organisationen zahlreiche unterschiedliche Technologien einsetzen, um alle Sicherheitsbedürfnisse abdecken zu können. Die Anforderung, alle Systeme miteinander zu verbinden, war noch nie so relevant wie heute. Cyber- und E-Mail-Attacken dienen als reichhaltige Quelle für Bedrohungsinformationen. Die Fähigkeit, diese Informationen zu erfassen und in das größere Sicherheitsökosystem zu integrieren, macht IT-Teams und ihre gesamten Sicherheitssysteme intelligenter.

Real-world scenario

Eine große Restaurantkette wurde regelmäßig mit Phishing-E-Mails ins Visier genommen, welche entsprechende Maßnahmen durch das IT-Team nach sich zogen, ein Prozess, der für jede E-Mail ein bis drei Stunden dauerte. Wie viel Zeit wurde für die Lösung dieses einzelnen Problems aufgewendet? Ungefähr 6500 Arbeitsstunden pro Jahr. Es musste einen effizienteren Weg geben, und die Integration der E-Mail-Sicherheitslösung (Mimecast) mit dem SOAR-Anbieter (Demisto) erwies sich als die Antwort. Durch die Integration der Suche nach Nachrichten, URL-Dekodierungund Absenderblockierung von Mimecast in Demisto konnte das Unternehmen den Zeitaufwand für die Behebung eines Phishing-Angriffs von 6500 Stunden pro Jahr auf nur 270 Stunden reduzieren.

Herausforderungen
Komplexe Security-Systemlandschaften
Nicht integrierte Plattformen und Technologien
Limitierte Transparenz über Systeme hinweg
Optimierung vorhandener Investments
Schlanke IT Abteilungen

Warum Mimecast, warum jetzt?

Mimecast stellt sich mit Email Security 3.0 den heutigen Herausforderungen an die E-Mail-Sicherheit. Unsere Technologie ist skalierbar und hilft Kunden, maximale Sicherheit zu erreichen und gleichzeitig Kosten und Komplexität zu reduzieren. Zahlreiche wichtige, dennoch unterschiedliche Technologien werden bei Mimecast in einer einzigen, leicht zu bedienenden Plattform zusammengeführt.

Gemeinsam stark

Wenn das Gerede über Technologie, Bedrohungen und Risiken verstummt, steht am Ende des Tages eine einfache Wahrheit im Vordergrund: Jedes Unternehmen ist mit der wachsenden Bedrohungslandschaft konfrontiert. Jede Organisation, ob groß oder klein, spielt eine Rolle in den digital vernetzten nationalen und globalen Ökosystemen, in denen wir heute leben und arbeiten. Als solche haben wir eine kollektive Verantwortung, zusammenzuarbeiten, um Cyber Attacken und Geschäftsbetriebsunterbrechungen zu verhindern, so dass “guten Unternehmen keine schlechte Dinge widerfahren”. Damit tragen wir zu dem größeren Ziel bei, eine globale Gemeinschaft von Regierungen, Unternehmen, Organisationen und Menschen aufzubauen, die ganz egal was noch an Cyber Bedrohungen auf uns zukommen wird, solide aufgestellt ist.