noSpamproxy®

CASE STUDY
E-MAIL SECURITY SUITE

Universitätsmedizin Essen stellt IT-Security neu auf und nutzt dafür NoSpamProxy

Klinikverbund setzt auf fortschrittlichste Technologien für bestmögliche IT-Sicherheit

Bei der Essener Universitätsmedizin (UME) handelt es sich um einen Klinikverbund, der neben dem Universitätsklinikum Essen 15 Tochterunternehmen umfasst – darunter die Ruhrlandklinik, das St. Josef Krankenhaus Werden, die Herzchirurgie Huttrop sowie das Westdeutsche Protonentherapiezentrum Essen. Mit etwa 11.000 Beschäftigten und 1.700 Betten ist die UME das führende Gesundheitskompetenzzentrum des Ruhrgebiets.

Bereits 2015 hat es sich der Verbund zum Ziel gesetzt, ein Smart Hospital zu werden – mit digitaler Bildgebung, Telemedizin aber auch dem Bereich Künstliche Intelligenz. Mittlerweile gehört die UME zu den smartesten Kliniken weltweit: auf einer Liste der Krankenhäuser, die sich die fortschrittlichsten Technologien zunutze machen – erstellt 2023 vom US-Magazin Newsweek in Zusammenarbeit mit der Online-Plattform Statista – hat es die Universitätsmedizin als eines von zwei deutschen Krankenhäusern unter die Top 20 geschafft.

Universitätsmedizin Essen
Universitätsklinikum

noSpam proxy®

Der Anspruch des Klinikverbunds, die technologisch fortschrittlichsten IT-Lösungen zu nutzen, erleichtert die Arbeit von Markus Bitter, Leiter der Stabsstelle Collaboration Software der UME, und seiner Kollegen ungemein: „Unser Ziel ist es, ein sicheres, einfach zu administrierendes digitales Zusammenarbeiten aller Bereiche der UME zu ermöglichen. Da ist es natürlich hilfreich, dass wir uns dafür die besten Lösungen am Markt aussuchen dürfen."

E-Mail Kommunikationsmittel Nummer 1 mit zahlreichen Herausforderungen

Nach wie vor ist die E-Mail für den Klinikverbund das bedeutendste Kommunikationsmedium, insbesondere in der externen Kommunikation. Pro Arbeitstag gehen ca. 45.000 E-Mails ein, davon werden etwa 15.000 abgelehnt, rund 8.500 Mails werden von der UME versandt. Verteilt auf zwei Rechenzentren, 53 Domänen und rund 13.200 Mailboxen ist so bisher eine E-Mail-Datenmenge von 54 TB entstanden. Laut Bitter hat die durchschnittliche E-Mail an der UME eine Größe von 400 KB. „Daran sieht man, dass an den heutigen E-Mails eigentlich immer ein Anhang ist und das ist für uns immer eine potenzielle Gefahr. Anhänge sind sicherheitstechnisch potenzielle Problemquellen, die wir uns anschauen müssen", schildert Bitter eine der größten Herausforderungen seines Teams.

Eine weitere enorme Herausforderung für das Unternehmen ist die Diskrepanz zwischen verschiedenen bindenden Compliance-Anforderungen wie Regularien des Gesundheitswesens, beispielsweise im Hinblick auf Vertraulichkeit, die DSGVO oder auch KRITIS-Vorgaben, und andererseits den unterschiedlichsten Einsendern von E-Mails. An die Universitätsmedizin Essen kommen Patienten mit Überweisungen aus Amerika oder Afrika, dazu treffen E-Mails mit Anhängen unterschiedlichster Formate ein, die in Deutschland kaum bekannt sind. Neben anderen Technologien gelten im Ausland auch andere Regularien. All das muss die IT der UME unter einen Hut bringen.

Hinzu kommt eine Vielzahl weiterer ganz alltäglicher Herausforderungen, die das Kommunikationsmedium E-Mail mit sich bringt: immer mehr Daten werden immer schneller übertragen, die Anwender erwarten, dass das Echtzeitmedium E-Mail genauso schnell ist wie die menschliche Sprache und ohne Verzögerung zugestellt wird, Links werden in E-Mails verteilt, oder Logins per E-Mail bestätigt. Parallel nutzen Kriminelle mit immer ausgefeilteren Attacken das Einfallstor E-Mail aus und die Nachrichten von angegriffenen Krankenhäusern, deren gesamte IT über mehrere Wochen lahmgelegt wird, häufen sich.

Besondere Herausforderungen

- Höchste Sicherheitsanforderungen gepaart mit Attraktivität als Angriffsziel
- Enorme Menge an eingehenden E-Mails mit verschiedenen Gefahrenquellen, insbesondere Anhängen
- Diskrepanz zwischen Compliance-Anforderungen und tatsächlich eingehenden E-Mails
- Anwender erwarten unmittelbare Zustellung
- Cyberangriffe werden immer raffinierter und häufen sich

Zunahme an Herausforderungen macht Neuaufstellung notwendig

2019 kam die IT der UME schließlich zur Überzeugung, die Fülle an immer weiter zunehmenden Herausforderungen mit den bisherigen Mitteln nicht mehr bewältigen zu können. Damals hatte der Verbund noch die E-Mail-Security-Lösung eines großen amerikanischen Herstellers im Einsatz mit dessen Support die UME trotz erheblicher Kosten nicht zufrieden war. Sie wollte sich deshalb bei der IT-Security komplett neu aufstellen. „Wir wünschten uns eine deutsche Lösung von Leuten, die uns verstehen. Einen coolen Hersteller und guten Partner dazu, der uns unterstützen und bei Bedarf auch mal für ein paar Tage Personal zur Seite stellen würde“, verdeutlicht Bitter die Anforderungen.

Zur weiteren Schärfung des Anforderungsprofils an eine neue Mail-Security-Lösung erstellte die interne IT eine E-Mail Policy, die unternehmensweit wie ein Gesetz gelten soll. Da sich mit NoSpamProxy Server alle Teile dieser Policy umsetzen ließen, war schnell klar, dass damit die richtige Lösung für die UME gefunden worden war.

Besondere Highlights

- Höchster Schutz auch im KRITIS-Umfeld – vom BSI nach BSZ zertifiziert
- Erfüllung sämtlicher Anforderungen und hohe Flexibilität
- IT der UME wird deutlich entlastet
- Zuverlässiger Support und kurze Reaktionszeit durch deutschen Hersteller

Quarantäne-Ordner abgeschafft

Zunächst schaffte die UME mit Unterstützung von NoSpamProxy die Quarantäne-Ordner ab. Bitter schildert die Aufbewahrung von E-Mails als extrem zeitfressend: die User müssten die Spam-Ordner durchsuchen, Admins müssten sie auf Schadsoftware oder Phishing prüfen, zudem nähmen sie Speicherplatz weg. Deshalb werden an der UME E-Mails entweder angenommen und zugestellt oder rigoros abgewiesen. „Wir machen 0 oder 1, wie sich das in der IT gehört“, so Bitter. Wenn eine E-Mail nicht zugestellt wurde, erhält der Absender eine Information darüber und kann reagieren.

> „Wir arbeiten sehr eng mit NoSpamProxy zusammen und wissen, dass wir im Fall der Fälle schnell jemanden in der Leitung haben, der sich um unser Problem kümmert. Außerdem schätzen wir den Austausch auf Augenhöhe sehr.
>
> Michael Drepper, ZIT, Stabsstelle Collaboration Software, Universitätsmedizin Essen

Individuelle Regeln für einzelne Kommunikationspartner

Ein zweiter wichtiger Punkt für die UME-IT waren die Partnereinstellungen. Grundsätzlich gelten für alle Beschäftigten des Unternehmens – von der Professorin bis zum Handwerker – die gleichen Regeln, jede und jeder hat die gleichen Rechte. Deshalb werden alle Ausnahmen, die die IT zulassen will, ausschließlich auf Absenderseite gewährt – entweder domainbasiert oder bezogen auf den konkreten Absender. Ein Beispiel hierfür sind E-Mails mit alten Office-97-Dokumenten im Anhang, die nur dann angenommen werden, wenn sie von einer bestimmten Domain

> Mit Net at Work haben wir einen Partner an unserer Seite, der alle unsere Anforderungen an eine zuverlässige und umfassende E-Mail-Lösung erfüllt.
>
> Dabei ist NoSpamProxy auch für ein Unternehmen unserer Größe einfach zu administrieren, was unsere IT spürbar entlastet.

Markus Bitter, Leiter Stabsstelle Collaboration Software, Universitätsmedizin Essen

aus verschickt werden. „Das war für uns ein echter Meilenstein, denn die Partnereinstellungen in NoSpamProxy sind ein Segen. Hier können wir ganz genau definieren, was ein Partner darf und was bei einem anderen Absender nicht erlaubt ist“, erläutert Bitter.

Moderne Inhaltsfilterung nach BSI-Grundschutz

Die Inhaltsfilterung, die auf den Empfehlungen des BSI-Grundschutzkatalogs basiert und vorgibt, wie mit verschiedenen Dateiformaten umgegangen werden sollte, ist ebenfalls ein wichtiger Baustein für das IT-Security-Konzept der Universitätsmedizin Essen. Die BSI-Empfehlungen wurden in vollem Umfang umgesetzt und werden sowohl im internen als auch externen E-Mail-Verkehr genau gleich angewandt: PDF geht immer durch, kritische Dateiformate werden immer abgelehnt – ganz gleich, ob sie innerhalb des Hauses verschickt werden oder von außen kommen.

Content Disarming und URL-Safeguarding schaffen weitere Sicherheit

Eine weitere Funktion, die bei der UME zum Einsatz kommt, ist das Content Disarming, das potenziell schädliche Inhalte wie beispielsweise ein altes Office-97-Dokument in ein sicheres PDF umwandelt. Die Erfahrung der UME-IT zeigt, dass die User in der Regel lediglich den Inhalt eines Dokuments sehen wollen und es nicht zwingend auch bearbeiten müssen. Deshalb reiche das umgewandelte PDF in den allermeisten Fällen aus.

URL Safeguard schließlich wandelt Links in E-Mails in einen internen Link um, bei dem bei jedem Draufklicken geprüft wird, ob er verseucht oder clean ist, bevor der Zugriff gewährt wird.

Robuste Lösung und umfassendes Know-how bieten Sicherheit und entlasten die interne IT

Mit NoSpamProxy kann die Universitätsmedizin Essen nicht nur ihre selbstgewählte E-Mail Policy vollumfänglich umsetzen, sondern profitiert von dem Experten-Know-how eines Herstellers, der die Sicherheitslage und Compliance-Auflagen im Krankenhausumfeld in Deutschland sehr gut kennt. Zudem profitiert die UME vom direkten Kontakt zu einem konkreten Ansprechpartner bei Net at Work und einem zuverlässigen und raschen Support.

NoSpamProxy bietet zuverlässigen Schutz vor Malware, Ransomware und Spam, erlaubt eine sichere und praxistaugliche E-Mail-Verschlüsselung, sorgt für den sicheren Versand großer Dateien und ermöglicht die mühelose zentrale Verwaltung von E-Mail-Disclaimern. Als erstes Softwareprodukt weltweit wurde NoSpamProxy vom Bundesamt für Sicherheit in der Informationstechnik (BSI) mit dem begehrten BSI-Zertifikat nach der Beschleunigten Sicherheitszertifizierung (BSZ) ausgezeichnet. Mit NoSpamProxy – als Cloud Service oder auf dem Server – erhalten Sie immer höchste E-Mail-Sicherheit „Made in Germany“. Mehr Informationen finden Sie online unter www.nospamproxy.com

Net at Work GmbH
Am Hoppenhof 32 A
33104 Paderborn
GERMANY
T +49 5251 304-800
F +49 5251 304-650
info@nospamproxy.com
www.nospamproxy.com