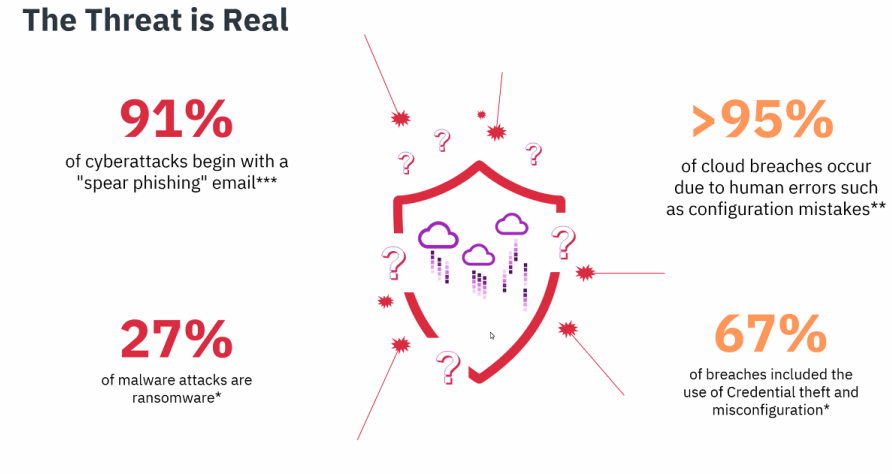
LIBRAESVA

Email Security Experts



Computing Security Award: beste Email Security des Jahres 2020 https://www.libraesva.com/computingsecurityawards2020/

Der erste Schutz gegen Ransomware und Phishing,
Unique Email-Sandboxing, Bitdefender integrierbar

Testen Sie Ihre Email Security: https://emailsecuritytester.com/ (dauert ca. 15 Minuten)
Und eignet sich auch hervorragend um die Office365 Security zu verbessern.

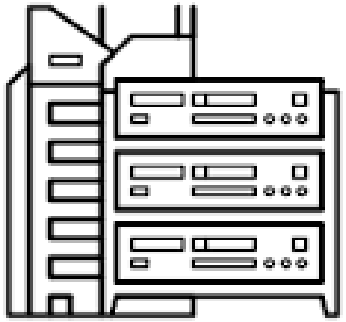
Referenzen: Fercam, Unidata, United Response, The Wirral College, Banca Popolare,

Integration mit u.a. Palo Alto

/LIBRAESVA

Deployment Options

On-premise



Public Cloud

Azure

aws

Libra Cloud

99.9%

24/7

aruba

UpCloud

The Libraesva Cloud Service is hosted in two DC's in Frankfurt, Germany. Compliant with ISO27001 & GDPR.

bsi. ISO/IEC 27001 Information Security Management

GDPR

Microsoft 365

Exchange

G Suite

zimbra

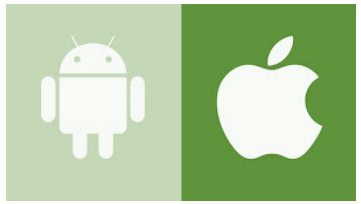
Lotus Domino

/LIBRAESVA

Product Suite

LIBRAESVA EMAIL SECURITY

- Security
- Continuity
- Encryption
- Data Loss Prevention



LIBRAESVA EMAIL ARCHIVER

- GDPR and Compliance
- Securely Store All Email
- Increase User Productivity
- Secure Third Parties Access

All Security Features and Technical Support **included in one License**
Purchased for 1/3/5 years

Why Libra?

Simplicity

Value for Money

Visibility

Excellent Detection Rates

virus BULLETIN 2010

Vendor	False Positives	False Positives (%)	Spam Catch Rate
Libraesva	6	0.27	99.95
Microsoft Forefront	5	0.23	99.93
The Email Laundry	12	0.55	99.79
Sophos	5	0.23	99.69
Bit Defender	3	0.14	99.55
Symantec	3	0.14	99.53
McAfee	11	0.5	99.33
Trustwave MailMarshal	5	0.23	99.14
Webroot	5	0.23	98.98
SpamTitan	3	0.14	98.52
Fortimail	5	0.23	98.01
Kaspersky	0	0	98.01

virus BULLETIN

2020-2021

Test Date	False Positives	Malware catch rate	Phishing Catch Rate
June-2020	0	99.73%	99.58%
Sept-2020	1	99.89%	99.43
Dec-2020	0	99.94%	98.81%
Mar-2021	0	100%	99.67%
Jun-2021	**1**	**100%**	**98.26%**

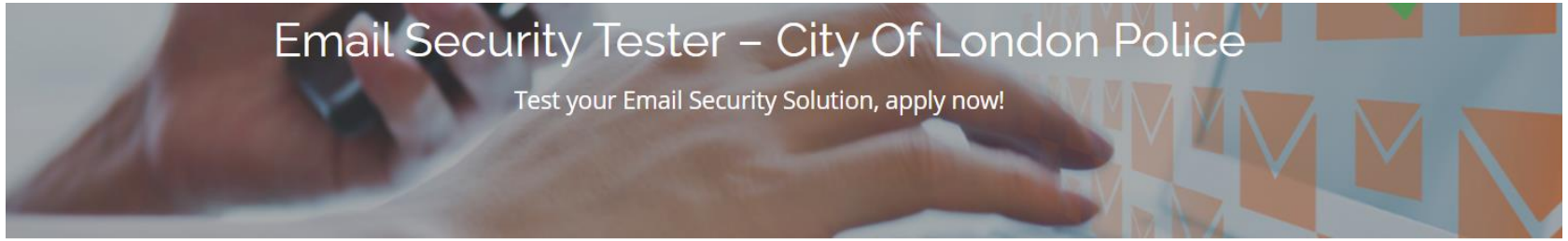

Widely Used by Corporate, Education, Finance and Government Departments in Germany
2500+ Installations Worldwide
Global Footprint
Features Designed Specifically for Education to Improve Safeguarding
69 Government Departments Protected
In 31 Countries
Our Cloud Service is hosted from 2 Datacentres in Germany
Awarded Best Email Security Solution 2014/15/16/17/19
Computer Security Awards
97% Customer Retention Rate
World Class Aftercare Support
/LIBRAESVA


Westerstede
Wohlfühlstadt im Grünen


RÖHDE


IFINA


ecos



Fields marked with an * are required

What is it about?

Over 90% of email traffic has spam, phishing, malware and other electronic threats. Email is the main infection vector for ransomware and malware.
This tool tests if your email server is correctly configured to stop these common threats.

How it works?

Just enter your email address below and we will send you a set of (totally harmless, but potentially) dangerous email; your security product should block or disinfect all samples sent to you.

Should some test email reach your inbox, don't jump to conclusions: read the email description to discover if and how the message has been disarmed.

Office 365 Users

The email security test works perfectly also with Microsoft Office 365. Please note that Microsoft is sending everything without any further analysis to the user's junk folder, so **cross check your junk folder** to confirm the test and to see which emails slipped through Microsoft filter.

- [x] Test Business Email Compromise (Whaling)

Whaling is a type of phishing fraud that targets high-profile end users such as C-level corporate executives, politicians and celebrities (hence the name Whaling). In order for the test to work, you have to specify the contact information for such users.

1. Spoofed envelope sender

Spoofing

Email spoofing is the creation of email messages with a forged sender address. Hackers use this technique to launch a phishing attack on as many employees as possible.

2. HTML analysis

Content

This email tests the ability of your Email Security Solution to detect threats in the message content. Some HTML tags are considered to be potentially dangerous to the extent that they can install ransomware.

3. Executable file

Attachment

Most email providers don't allow you to send executable or ".exe" files. Most executable files are legitimate. However, some executable files are malicious and used to spread malware. Attached you'll find a widely well-known executable file, absolutely harmless, named putty.exe.

4. Virus attachment

Attachment

This is a well-known code, known by all antivirus, which is used for the purpose of testing that the antivirus is functional and reacting to signature-based virus.

5. Outlook Conditional Comment

Content

This email tests the ability of your email security solution to detect threats in the message content. Microsoft Outlook for Windows uses HTML comments as the conditional rendering engine. That means an attacker could exploit this feature by storing, for example, bad links in comments that are usually ignored by other email clients, targeting Microsoft Windows clients.

6. Malware URI

Link

This email tests the ability of your Email Security Gateway to detect hidden malware URI's in realtime, so that 0-day and 0-hour threats can be blocked as soon as they are detected.

7. Zero Width Spaces link

Link

The zero width space (ZWSPs) is an Unicode character. It's white space but renders with zero width. So you don't see it. This email tests the ability of your Email Security Gateway to detect zero width spaces (ZWSPs) used in links to bypass security features.

8. Base HTML Tag link

Link

This email tests the ability of your Email Security Gateway to detect a vulnerability known as baseStriker that allows miscreants to send malicious emails that bypass security systems.

9. HTML JS Redirect Attachment

Attachment

Recently in the wild .HTML file attachments have been used to deliver malcode (usually via embedded Javascript) to endpoints. That's why your Email Security Gateway should look at this trick and protect you by removing or disarming the .HTML attachment.

10. RFC-Abused HTML Attachment

Attachment

A Request for Comments (RFC) is a formal document from the Internet Engineering Task Force (IETF) that are considered Internet standards. If your email script's coding is not RFC compliant, a mail servers should reject the email.

11. Active PDF

Attachment

Adobe PDF Reader (and possibly other readers) contains a Javascript engine similar to the ones used by web browsers. This means that PDF documents are not purely static, and for example some actions may be used to fool a user (popups) or to send e-mails and HTTP requests automatically. Furthermore, experience shows that many recent vulnerabilities have been exploited using Javascript in PDF.

12. PDF with malicious text link

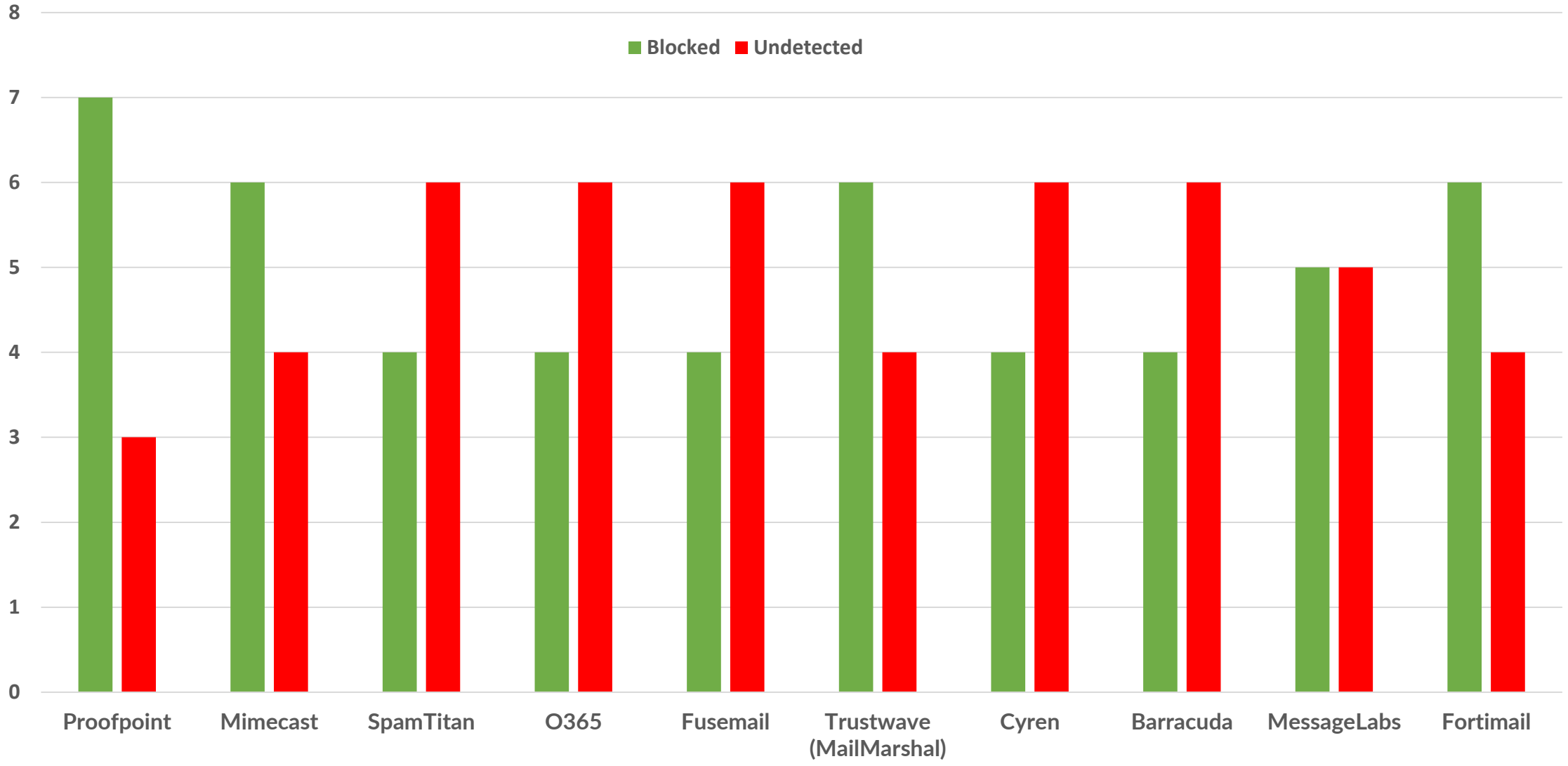
Attachment

PDF files can contain text, images and links. Or.. what we call a text link, that is normal text pointing to a website. Adobe Reader (and possibly other readers) with the goal of making the life easier to users, automatically detects such text links making them active so you can just click on the link.

Including Testing against (BEC)

Business Email Compromise is a type of phishing fraud that targets high-profile end users such as C-level corporate executives, politicians and celebrities. **Email impersonation attacks** — also known as **CEO fraud** or **whaling attacks** — are a growing concern for organizations of any size. If you want to test your protection against it we need some more information about a person we will try to impersonate (The Whale).

Email Security Pen Test Results



Licencing

Standard License includes all security features and technical support *(8am-6pm CET, Mon-Fri, phone and email direct).*

- For Office365 and Gsuite users, the product is licensed by number of active users in the 365/Gsuite tenant.
- For any other mailserver (exchange/Zimbra etc), the product is licensed by number of email addresses (including shared mailboxes, distribution groups and aliases.
- Purchased on 1/3 or 5 year subscription

Additional options include Bit Defender and Avira Antivirus Engines, End to end encryption, Policy Quota (rate limiting the number of emails that can be sent) and Clustering (for high availability active-active cluster) and URLsand white labelling. The licenses amount must match the quantity licenses for the Libraesva Email Security Subscription and are charged additionally but are Optional.

MSP License

Libraesva also includes an MSP offering. This will provide an MSP with a multi-tenanted, fully whitelabellable service to manage all of your clients from one Libraesva Email Security Solution with granular configurations for individual management of each organisation.

The MSP platform is Licensed, per email address (which should include shared mailboxes, distribution groups but Aliases are included at no additional charge) for 90 days (billed quarterly). You can move up and down the licence brackets every quarter. The more mailboxes on the platform the lower the cost per mailbox. Price breaks include; 500, 1000, 1500, 2000 etc. During the 90 days you can onboard as many new clients and we will not backdate or charge for the overuseage.

Our Email Archiving service follows the same model but is licensed by storage required.

Email Risk Assessment - POC Report

77% of your email traffic is malicious or unwanted content.

Analysing your organisations email traffic allows us to understand how many of the emails you are receiving are legitimate and helps to justify whether an additional layer of security is needed.

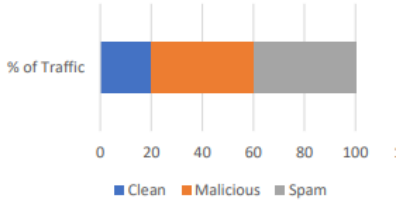
The data below shows that a significant portion of your businesses email traffic was categorised as malicious or unwanted email. The average amount of spam received is around 30%.

Time Period: **6 months**

Number of emails received: **1,109,081**

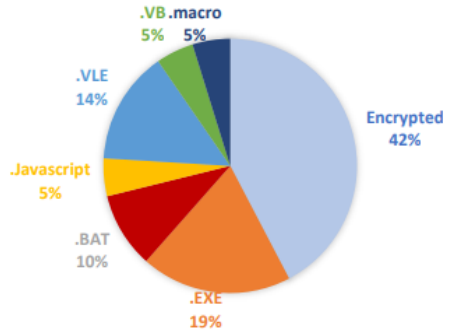
Number of Spam emails received: **684,072**

Number of malicious emails received: **138,011**



40+ malicious file types found in 100,000+ emails.

Email security solutions are designed to filter out malicious and unwanted content and stop these emails from ever reaching the users mailboxes. Understanding the types of threats you are receiving helps to justify the level of protection you need to employ, as a minimum, based on the threats that have already been targeting your organisation.

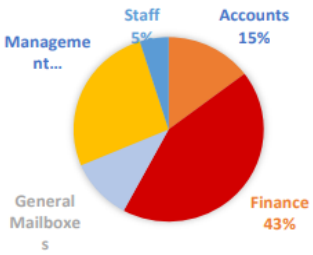


Exploited Applications:

1. Mailchimp
2. OneDrive
3. Zoom
4. GoogleDrive
5. DropBox

Accounts, finance and management targeted by 84% of threats.

Understanding which departments are being targeted by threats provides valuable insight into who cybercriminals are targeting your organisation.



Distribution of threats within your organisation shows that the Finance department is being targeted substantially more than others. This is generally due to the nature of that department and financially driven motivates of the cybercriminals.

Senior management provide a way for attackers to leverage the trust and authority by impersonating their email addresses and contacting other areas of the business.

Phishing attempts were highly targeted and financially motivated.

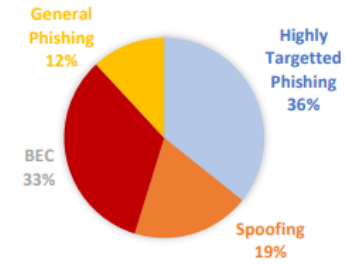
By looking at a breakdown of the types of phishing attacks you are receiving, we can gain further insight into how cybercriminals are targeting your organisation and their motivations.

The data shows a high quantity of impersonation and spoofing attempts were made on authoritative figures within your organisation. A significant portion of phishing emails detected are being carefully crafted and specifically targeted towards certain individuals.

Number of Phishing emails blocked: **208,012**

Spoofing Attempts blocked: **68,077**

Impersonation attempts: **50,003**



Thank you for Listening, Any Questions?