Fragen und Antworten (FAQ) zu E-Mail (Outlook) und anderen externen Daten(-trägern)

Jeden Tag bekommen wir alle E-Mails von unterschiedlichsten Absendern. Viele dieser E-Mails sind für das tägliche Geschäft notwendig, aber es stecken auch Mails dazwischen, die wir nicht bekommen wollen. Manchmal ist es einfach nur Werbung, die nur lästig ist und nach Sichtung einfach gelöscht werden kann. Es steckt aber durchaus auch Gefahr in solchen E-Mails. So kann es durchaus sein, dass in einer solchen E-Mail ein Anhang steckt, der sehr gefährlich ist. Kriminelle versuchen auf diesem Weg an unsere Daten oder an Geld zu kommen. Es kann beispielsweise in diesem Anhang ein ausführbares Programm stecken, welches dann auf Ihrem Rechner oder auf Servern, auf die Sie Zugriff haben, Schaden anrichten oder Daten abgreifen, die Sie nicht weitergeben wollen. Man spricht dann von sogenannter Schad-Software (engl. Malware). Es gab bereits Vorfälle bei denen Kriminellen Daten des Unternehmens verschlüsselt haben und dann dieses erpressen. Gegen Zahlung einer sehr hohen Summe wird versprochen die Daten wieder freizugeben. All diese Art von unerwünschtem Mailverkehr nennt man auch SPAM. Aus diesem Grund mussten wir auch ZIP Dateien vorübergehnd blockieren, was in einigen Bereichen zu Mehraufwand geführt hat. Nun konnten wir den Filter jedoch optimieren und ausgehende Archiv-Dateien wieder zulassen und stellen diese direkt zu.

MSP versucht im Vorfeld systemseitig bzw. automatisiert diesen SPAM und insbesondere Schad-Software, zu filtern. Aufgrund der vielen unterschiedlichen Formen von SPAM kann aber nicht alles gefiltert werden. Wären wir zu rigoros, blieben auch zu viele E-Mails im Filter hängen, die weder Schaden anrichten, noch problematisch sind und dann würden sehr viele E-Mails hängen bleiben, die Sie erwarten bzw. benötigen. Daher muss jeder auch ein Auge auf die E-Mails und den Inhalt haben, bevor man einfach "klick" macht. Denn wenn ein Anhang geöffnet wird, dann kann es bereits passiert sein.

Frage	Antwort
Wie erkenne ich E-Mails mit gefährlichem Inhalt?	**Bekommen Sie E-Mails, die Sie nicht erwarten oder deren Absender Ihnen unbekannten ist, klicken Sie diese nicht einfach an.** Wichtig ist, immer die Augen offen halten und bei Unsicherheit lieber einmal zu vorsichtig zu sein, als einmal zu wenig. Lassen Sie die E-Mail lieber liegen oder fragen den Absender telefonisch, ob er Ihnen die Mail wirklich geschickt hat. Fragen Sie auch gerne einen Kollegen um Rat oder rufen den MSP Support an. Erst wenn Sie sich sicher sind, öffnen Sie die E-Mail bzw. den Anhang. Mit ein paar einfachen Maßnahmen können Sie gefährliche E-Mails oft bereits erkennen ... • Kriminelle versuchen gerne Ihnen vorzutäuschen, das die E-Mail von einem bekannten Absender kommt. Gehen Sie mit der Maus (WICHTIG: ohne zu klicken) einfach mal über den Absender, taucht nun eine bekannte E-Mail-Adresse auf oder steht da doch was ganz anderes? Ist die Domain (der Teil nach dem @-Zeichen) korrekt geschrieben? Gerne wird auch vorzutäuschen versucht, dass der Absender ein großer Dienstleister ist. Amazon, Paypal, etc. verwenden immer ihre Haupt-Domain als Mail-Adresse, niemals jedoch mit Erweiterungen (falsch wäre z.B. @amazon-service.de, @service-paypal.com). E-Mails mit derartigen Absendern sollte man sofort löschen! • Links auf andere Webseiten bergen Gefahren. Insbesondere wenn diese auf Webseiten zeigen, die nicht zum Anbieter gehören. Auch hier gilt die Regel von oben, die großen Dienstleister verweisen immer auf ihre eigenen Haupt-Domains und haben niemals Service-Seiten mit andern Domains. Fahren Sie auch hier einfach mal - ohne zu klicken - über den Link. Stimmt der Link mit dem angezeigten überein? Wenn das nicht stimmt, dann auf keinen Fall anklicken! • Sind gravierende Tippfehler, Formulierungsfehler oder grammatikalische Fehler in der Mail? Oft ist auch das ein Anzeichen auf eine unsaubere Herkunft. Das ist zwar kein sicheres Anzeichen, zumal die online verfügbaren Übersetzungsdienste immer besser werden. Ist die E-Mail dennoch schlecht übersetzt und es stecken Links oder Anhänge in der E-Mail, dann ist Vorsicht geboten. • Steckt in der E-Mail ein Anhang vom Typ einer Office-Datei (DOCX für Word, XLSX für Excel, PPTX für PowerPoint), dann ist besondere Vorsicht geboten. Diese Dateien können ausführbaren Code, sogenannte Makros oder Visual Basic Code für Anwendungen (VBA) enthalten. Office-Programme waren mit einem Hinweis bzw. der Frage ob dieser geöffnet werden soll. Dieser Code ist ein erhebliches Risiko und, selbst wenn der Absender bekannt ist, darf dieser nicht ausgeführt werden. Sie können nicht erkennen, was der Code macht und ob dieser ggf. noch Daten bzw. Schad-Software aus dem Internet herunterlädt. Ist dieser Code notwendig, lassen Sie das unbedingt vorher von jemandem untersuchen und freigeben. Wir stehen in diesen Fällen gerne zur Verfügung. • Steckt in der E-Mail eine Rechnung und Sie haben mit dem Unternehmen noch nie eine Geschäftsbeziehung gehabt, dann stimmt da was nicht. Warum sollte man Ihnen eine Rechnung schicken? Würde diese nicht eher an den Einkauf oder eine andere Person des Unternehmens gehen? Bitte diesen Anhang nicht ohne weitere Prüfung oder Rückfrage öffnen. • Steckt in der E-Mail ein Anhang in Form einer ZIP-Datei und das Kennwort der ZIP-Datei ist (praktischerweise) gleich in der E-Mail, dann ist das zumindest mal merkwürdig. Würden Sie eine Geldkassette verschicken und den Schlüssel mit einem Streifen Tesa auf die Kassette kleben? Es ergibt keinen Sinn, den Schlüssel auf demselben Weg zu versenden wie den schützenswerten Inhalt, erst Recht ergibt es keinen Sinn diesen gleich dabei zu packen. Sollten Sie eine derartige E-Mail erhalten, war der Absender im einfachsten Fall nur Dumm, meistens will er Sie aber täuschen und hofft, dass Sie auf diesen Trick hereinfallen. Löschen Sie diese Mail besser, sicher sind die Daten sowieso nicht. • Darlehensangebote, Gewinnzusagen, etc. kommen nicht bei Ihnen an, wenn Sie dieses nicht angefordert haben oder wenn Sie an einem Preisausschreiben teilgenommen haben. Niemand hat etwas zu verschenken. Menschen, die so freundlich scheinen, wollen Ihr Geld oder das Geld Ihres Unternehmens, zumindest aber Ihre Daten. Das sind jetzt nur ein paar Hinweise SPAM zu erkennen, es gibt täglich neue Formen, daher muss man immer die Augen offen halten und nichts anklicken, was komisch aussieht. Sind Sie sich unsicher, rufen Sie den Absender einfach über die Ihnen vorher bereits bekannte Telefonnummer, nicht aber über die aus der E-Mail, an und fragen, ob er Ihnen diese E-Mail wirklich geschickt hat und ob der Anhang dabei sein sollte.

Was mache ich, wenn ich doch eine E-Mail angeklickt habe, die ich besser nicht angeklickt hätte?	**Sollte es doch passiert sein, dann ist Eile geboten!** Zuerst nehmen Sie den Rechner sofort vom Netzwerk, ziehen sofort alle Stecker und trennen den Rechner vom WLAN. Da das manchmal aber einfach zu lange dauern kann, schalten Sie ihn einfach aus. Bei Notebooks reicht das Ziehen des Steckers vom Netzteil nicht aus, diese Geräte laufen ja auch ohne Stromversorgung weiter. Hier hilft es den Hauptschalter lange zu drücken. In der Regel drückt man diesen für 10 Sekunden und das Gerät geht einfach, ohne herunterzufahren, aus. Damit ist erstmal nur erreicht, dass der Schadcode nicht mehr läuft. Dieses Gerät darf aber in keinem Fall wieder eingeschaltet werden, dann startet der Code mit hoher Wahrscheinlichkeit wieder. Lassen Sie das Gerät ausgeschaltet! Rufen Sie danach sofort bei uns im Service (+49-421-9579-7777) an. Wir kümmern uns um ein Ersatzgerät für Sie und untersuchen Ihren Rechner bzw. betanken diesen dann neu.
Wie groß dürfen Anhänge (Dateien) an E-Mails sein?	Die maximale Größe von E-Mails inkl. Anhang, die auf die von MSP betriebenen Mailserver zugestellt werden kann, darf 70 MB nicht überschreiten. Nun werden Anhänge an E-Mail jedoch kodiert übertragen und werden für den Transport größer als die eigentliche Datei ist. Daher darf an einer Mail max. 50 MB angehängt sein. Dieser Wert gilt für alle Anhänge zusammen.
Welche Anhänge (Datei-Typen) an E-Mails sind zulässig? Warum werden Anhänge nicht zugestellt?	Wir blocken aktuelle alle potenziell gefährliche Inhalte. Dazu gehören insbesondere: • Ausführbare Dateien (EXE, JAR, usw.) • Office mit Makros • ausgehende Archive (ZIP, RAR, 7ZIP, TAR usw.) • Multimedia-Dateien (Flash, AVI, MPEG usw.) Je nach Bedrohungslage kann diese Liste jederzeit erweitert werden.
Wie kann ich mir Anhänge zustellen lassen, die vom Mailsystem geblockt wurden? Wie groß dürfen diese Dateien sein?	Kriminelle versuchen, ohne individuellen Aufwand möglichst viele Adressaten zu erreichen. Daher ist E-Mail auch genau das Mittel der Wahl um Schadcode zu versenden. Daten auf einer Webseite einzustellen ist ungleich aufwendiger. Bei der Verwendung eines Captcha ist das Hochladen von Dateien kaum noch automatisierbar. Ein Captcha ist z.B. ein Bild, indem auf unsauberer Fläche Buchstaben und Zahlen in unterschiedlich formatierten Buchstaben stehen, die Sie abtippen müssen oder eine Bildersammlung, auf der Sie nach Objekten (z.B. Brücken oder Ampeln) suchen müssen und diese Bilder dann markieren müssen. MSP stellt ein Portal bereit, über das man Ihnen Dateien zukommen lassen kann. Wird eine Datei, die Ihnen per E-Mail zugestellt werden soll, und die Sie dringend benötigen und erwarten, geblockt, können Sie dem Absender die URL https://webupload.medien-systempartner.de/ zusenden. Der Absender kann auf diesem Portal Dateien bis zu einer maximalen Größe von 500 MB einstellen, seine eigenen Daten inkl. einer kurzen Nachricht eingeben und Ihnen diese Daten an Ihre E-Mail Anschrift schicken lassen. Sobald die Daten hier eingestellt wurden, werden diese im Hintergrund über einen weiteren Virenscanner geleitet und Ihnen per E-Mail zugestellt. Auf diesem Portal können aber nur E-Mail Domains für Empfänger verwendet werden, die intern registriert sind.
Mein Postfach ist voll, was kann ich selbst tun?	Am einfachsten ist es alte E-Mails zu löschen. Outlook stellt hierzu auch Werkzeuge bereit. Man kann z.B. unter Datei / Tools den eigenen Papierkorb löschen. Oft steckt da schon sehr viel an zu löschenden E-Mails drin, die aber immer noch Platz verbrauchen. Reicht das immer noch nicht aus, kann man über die Postfachbereinigung einen Blick auf die effektive Größe des eigenen Postfachs und aller Unterordner werfen. Ordner, die unterhalb des Eingangsordners angelegt werden, sind immer noch Bestandteil des Postfachs. Daher kann man auf diese ja auch mobil und über den Webbrowser zugreifen. Outlook bietet aber auch den Weg einer Archvierung oder der automatischen Lösung älterer Inhalte. Archiv-Dateien sind sogenannte PST Dateien. Diese sollte man auf keinem Fall auf Server-Laufwerken ablegen, wenn man diese dauerhaft in Outlook einbinden möchte. Outlook wird dann langsam uns instabil. Zur dauerhafen Archivierung kann man diese ausgelagerten Daten aber zurück auf den Server verschieben um diese Daten auch in der täglichen Datensicherung zu haben. Speichern Sie diese Daten daher zunächst auf dem Laufwerk C:, am besten in Ihrem Profil unter Dokumente oder Outlook-Dateien und verschieben bzw. kopieren diese dann nach erfolgter Archivierung auf ein zentrales Laufwerk. Sind Sie bereits Nutzer von OneDrive (ein Bestandteil von Office 365), sichern Sie diese Daten auf ihrem persönlichen OneDrive Ordner. Dieser wird automatisch synchronisiert und ist von Outlook unterstützt.
Was muss ich bei der Nutzung von USB Sticks beachten?	Benutzen Sie keine USB-Sticks und andere Datenträger, wie z.B. USB Disks, CDs, etc., von unbekannten Quellen bzw. nicht vertrauenswürdiger vorheriger Verwendung. Verwenden Sie ausschließlich externe Datenträger, bei denen Sie sicher sein können das diese auch sauber sind. Im Zweifelsfall stellen Sie bitte ein JIRA Ticket zur Untersuchung des Datenträgers ein und geben Sie den Datenträger zur Untersuchung bei MSP im Service ab. Die Kollegen überprüfen diesen dann unter Laborbedingungen und spielen Ihnen die Daten auf einen sicheren Speicherplatz ein.