TLP:GREEN

Bundesamt
für Sicherheit in der
Informationstechnik

Bundesamt für Sicherheit in der Informationstechnik, 55133 Bonn

Versand als Anlage zur Cyber-Sicherheitswarnung

An die Bundesländer und Institutionen der Wirtschaft

Nationales IT-Lagezentrum
Bundesamt für Sicherheit in der Informationstechnik

Godesberger Allee 185-189
53175 Bonn

Postanschrift:
Postfach 20 03 06
53133 Bonn

Tel. +49 228 99 9582-5110

lagezentrum@bsi-bund.de

www.bsi.bund.de

Betreff: Maßnahmen zum Schutz vor Schadprogramm-Infektionen mit Emotet/Trickbot

Bezug: Cyber-Sicherheitswarnung
Geschäftszeichen: 210 04 02 1219-2
Datum: 22.01.2020
Seite 1 von 30
Anlage: Maßnahmenkatalog

Das Bundesamt für Sicherheit in der Informationstechnik hat mit dem beigefügten Maßnahmenkatalog eine Sammlung von möglichen (zentralen) Schutzmaßnahmen – vor weiteren möglichen EMOTET-Wellen - erstellt.
Es wurde kurzfristig eine große Bandbreite von möglichen Maßnahmen zusammengestellt und mit strukturierenden, bewertenden und umsetzungsorientierten Informationen versehen. Dazu zählt ein Priorisierungsangebot durch die Reihenfolge auf Basis der Kurzfristigkeit der Umsetzung. Aber auch die Wirksamkeit sowie die Konsequenzen und "Nebenwirkungen" der Maßnahmen.

Primär liegt die Entscheidung zur und die tatsächliche Umsetzung in Ihrem Zuständigkeitsbereich. Nutzen Sie für die Umsetzung ggf. Ihren IT-Dienstleister. Das BSI kann hierbei keine Einzelfallunterstützung bieten. Gerne bündeln wir Fragen und versuchen den Maßnahmenkatalog dann geeignet weiter zu ergänzen.

Bitte beachten Sie, dass einige der Maßnahmenkonsequenzen sehr massiv sind. Sie kommen eher als Notfallmaßnahmen bei einer weiteren Eskalation der Lage in Betracht.

Bundesamt
für Sicherheit in der
Informationstechnik

Hinweis:
Da der Maßnahmenkatalog kurzfristig erstellt wurde, erhebt er keinen Anspruch auf Vollständigkeit und "überprüfte Richtigkeit". Er wurde als kurzfristige Reaktion erstellt.

Auch ersetzt die Umsetzung dieser Punkte nicht die generellen Empfehlungen des IT-Grundschutzes sowie anderer Richtlinien und Vorgaben welche auf Sie zutreffen.

Mit freundlichen Grüßen,
Im Auftrag

Ritter

Bundesamt
für Sicherheit in der
Informationstechnik

Maßnahmenkatalog

Inhalt

Hinweis zu den in diesem Dokument verwendeten Links

Alle Links in diesem Dokument wurden verfremdet. Hintergrund dieser Maßnahmen sind Schutzmaßnahmen in Institutionen, die Links in Dokumenten verbieten.
Zur Nutzung der Links entfernen Sie bitte die eckigen Klammern ([ ]).
https[:]//www[.]ichbineinlink[.]de → https://www.ichbineinlink.de

Bundesamt
für Sicherheit in der
Informationstechnik

I. (Plan-) Besprechung zur Reaktionsvorbereitung

Schulnote Wirksamkeit	1
Schulnote Umsetzbarkeit	2
Schulnote Risiken	2
Maßnahmentitel	Planbesprechung zur Reaktionsvorbereitung
Maßnahmenbeschreibung	Durchführung einer Planbesprechung unter Mitwirkung der IT-Sicherheit (ISB), der IT / des IT-Dienstleisters, der Unternehmensführung, der Presse- und Medienverantwortlichen, etc. Die Planbesprechung soll thematisieren, welche Maßnahmen ergriffen werden, wenn eine EMOTET-Infektion in der eigenen Institution vorliegt und - Daten abfließen - Malware-Spam im Namen der Institution verteilt wird - Trickbot oder andere Schadsoftware nachgeladen wird
Wirkstelle der Maßnahme	Präventionsmaßnahme
Notwendige Voraussetzungen	Information der Unternehmensführung
Material / Links / Hilfen	Lesen Sie die Dokumente und prüfen sie die Umsetzung der beschriebenen Maßnahmen. Sensibilisieren Sie die MitarbeiterInnen bezüglich der EMOTET-Welle und dem Umgang mit Phishingmails. Planen Sie den Umgang mit zahlreichen Phishingmails in den persönlichen Posteingängen. Planen Sie den Infektionsfall und prüfen sie die vorhandenen Schutzmaßnahmen (vor allem in Bezug auf ADs, Backups, etc.). Überlegen Sie auch, welche Aufgaben die Mitarbeiter bei einem (möglicherweise) mehrwöchigem Ausfall von IT-Systemen ausführen können. Stellen Sie sich darauf ein, dass diese Bedrohung mittelfristig nicht zurückgehen wird.
Risiken und Nebenwirkungen	

II. Header-Antispoofing I

Schulnote Wirksamkeit	2
Schulnote Umsetzbarkeit	1
Schulnote Zeitaufwand	1
Schulnote Risiken	4
Maßnahmentitel	Header-Antispoofing
Maßnahmenbeschreibung	Schärfung der Header-Antispoofing-Regeln, so dass aus dem Internet eintreffende E-Mails mit gefälschtem Absender immer als Spam markiert werden oder in eine Quarantäne aussortiert werden
Kann es in jeder Institution, an den Netzübergängen, für mehrere Institutionen (DL) umgesetzt werden	am Netzübergang vom Internet zum Netz der Institution
Notwendige Voraussetzungen (System, Tool, Programm, Produkt, ...)	Verwendung eines Spamfilters
Material / Links / Hilfen / Beschreibungen wie umsetzbar	Umsetzung nach den eigenen Regeln der Institution
Risiken und Nebenwirkungen, was passiert wenn umgesetzt, was geht dann wahrscheinlich nicht mehr	Header-From-Spoofing wird bei sehr vielen erwünschten Mails gemacht (z.B. bei Newslettern). Diese würden dann auch markiert und ggf. aussortiert.

Bundesamt
für Sicherheit in der
Informationstechnik

III. Header-Antispoofing II

Schulnote Wirksamkeit	2
Schulnote Umsetzbarkeit	1
Schulnote Zeitaufwand	1
Schulnote Risiken	3
Maßnahmentitel	Header-Antispoofing II
Maßnahmenbeschreibung	Schärfung der Header-Antispoofing-Regeln, so dass aus dem Internet eintreffende E-Mails mit institutions-internen Domains im Header-From immer als Spam markiert werden oder in eine Quarantäne aussortiert werden
Angriffs- / Infektionsvektor	
Wirkstelle der Maßnahme	
Kann es in jeder Institution, an den Netzübergängen, für mehrere Institutionen (DL) umgesetzt werden	am Netzübergang vom Internet zum Netz der Institution
Notwendige Voraussetzungen (System, Tool, Programm, Produkt, ...)	Verwendung eines Spamfilters
Material / Links / Hilfen / Beschreibungen wie umsetzbar	Umsetzung nach den eigenen Regeln der Institution
Risiken und Nebenwirkungen	mäßiger Kollateralschaden
Risiken und Nebenwirkungen, was passiert wenn umgesetzt, was geht dann wahrscheinlich nicht mehr	Header-From-Spoofing mit institutions-internen Absendern wird von einigen Institutionen mit externen Dienstleistern gemacht. Diese würden dann auch markiert und ggf. aussortiert.

Bundesamt
für Sicherheit in der
Informationstechnik

IV. Quarantänisierung aller aus dem Internet eingehender E-Mails mit Office-Dokumenten

Schulnote Wirksamkeit	1
Schulnote Umsetzbarkeit	1
Schulnote Zeitaufwand	1
Schulnote Risiken	4
Maßnahmentitel	Quarantänisierung aller aus dem Internet eingehender E-Mails mit Office-Dokumenten
Maßnahmenbeschreibung	Quarantänisierung aller aus dem Internet eingehender E-Mails mit Office-Dokumenten. Derzeit wird Emotet hauptsächlich über Office-Dokumente verteilt (sofern keine Links verwendet werden). Sollte dies wie Anfang 2019 erfolgen müsste hier nachgesteuert werden.
Kann es in jeder Institution, an den Netzübergängen, für mehrere Institutionen (DL) umgesetzt werden	am Netzübergang vom Internet zum Netz der Institution
Notwendige Voraussetzungen (System, Tool, Programm, Produkt, ...)	Verwendung eines Spamfilters
Material / Links / Hilfen / Beschreibungen wie umsetzbar	Umsetzung nach den Regeln der Institution
Risiken und Nebenwirkungen	erheblicher Kollateralschaden
Risiken und Nebenwirkungen, was passiert wenn umgesetzt, was geht dann wahrscheinlich nicht mehr	Institutionen können keine Office-Dokumente von externen Partnern empfangen.

Bundesamt
für Sicherheit in der
Informationstechnik

V. Quarantänisierung aller institutions-internen E-Mails mit Office-Dokumenten

Schulnote Wirksamkeit	1
Schulnote Umsetzbarkeit	1
Schulnote Zeitaufwand	1
Schulnote Risiken	4
Maßnahmentitel	Quarantänisierung aller institutions-internen E-Mails mit Office-Dokumenten
Maßnahmenbeschreibung	Quarantänisierung aller institutions-internen E-Mails mit Office-Dokumenten. Derzeit wird Emotet hauptsächlich über Office-Dokumente verteilt (sofern keine Links verwendet werden). Sollte dies wie Anfang 2019 erfolgen müsste hier nachgesteuert werden.
Notwendige Voraussetzungen (System, Tool, Programm, Produkt, ...)	
Material / Links / Hilfen / Beschreibungen wie umsetzbar	Umsetzung nach den Regeln der Institution
Risiken und Nebenwirkungen	erheblicher Kollateralschaden
Risiken und Nebenwirkungen, was passiert wenn umgesetzt, was geht dann wahrscheinlich nicht mehr	Institutionen können keine Office-Dokumente von externen Partnern oder anderen Institutionen empfangen

Bundesamt
für Sicherheit in der
Informationstechnik

VI. Applikations-Whitelisting mit Applocker

Schulnote Wirksamkeit	1
Schulnote Umsetzbarkeit	1
Schulnote Zeitaufwand	1
Schulnote Risiken	2
Maßnahmentitel	Applikations-Whitelisting mit Applocker
Maßnahmenbeschreibung	Umsetzung von Applocker mit Standard-Regeln
Angriffs- / Infektionsvektor	Nachladen der Schadsoftware nach Kontakt mit dem C2 Server
Wirkstelle der Maßnahme	Betriebssystem
Kann es in jeder Institution, an den Netzübergängen, für mehrere Institutionen (DL) umgesetzt werden	Ja nein nein
Notwendige Voraussetzungen (System, Tool, Programm, Produkt, ...)	Nutzung von Windows in der Enterprise-Edition (in der Pro-Version nur Audit-Mode möglich) Zur besseren Lageeinschätzung ist es empfehlenswert die Ereignis-ID 8003 und 8004 zu überwachen, die Überwachung funktioniert bereits ab der Windows Professional-Edition. Erklärung der Event-IDs: https[:]//docs[.]microsoft[.]com/de-de/windows/security/threat-protection/windows-defender-application-control/applocker/using-event-viewer-with-applocker
Material / Links / Hilfen / Beschreibungen wie umsetzbar	BSI Grundschutz SYS.2.2.2.A14 Anwendungssteuerung mit Software Restriction Policies und AppLocker(CIA) https[:]//www[.]bsi[.]bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/bausteine/SYS/SYS_2_2_2_Clients_unter_Windows_8_1[.]html BSI CS 117: Sicherer Einsatz von Microsoft AppLocker https[:]//www[.]allianz-fuercybersicherheit[.]de/ACS/DE/_/downloads/BSI-CS/BSI-CS_117[.]pdf Microsoft AppLocker Design Guide
Risiken und Nebenwirkungen, was passiert wenn umgesetzt, was geht dann wahrscheinlich nicht mehr	Legitime Programme, die sich nicht an die Design-Vorgaben von MSFT halten, können bis zur Anpassung der Regel nicht mehr genutzt werden.

Bundesamt
für Sicherheit in der
Informationstechnik

VII. Sperrung des Zugriffs auf bekannte auf Emotet-Download-URLs

Schulnote Wirksamkeit	3
Schulnote Umsetzbarkeit	2
Schulnote Zeitaufwand	2
Schulnote Risiken	2
Maßnahmentitel	Sperrung des Zugriffs auf bekannte auf Emotet-Download-URLs
Maßnahmenbeschreibung	URLhaus stellt aktuelle Informationen zu bekannten URLs bereit, welche in Emotet-Spams enthalten sind (https[:]//urlhaus[.]abuse[.]ch/browse/). Eine Sperrung des Zugriffs auf diese URLs verhindert den Download der schädlichen Office-Dokumente, wenn ein Nutzer den Link anklickt. Die Wirksamkeit dieser Maßnahme ist stark von der Einspielgeschwindigkeit abhängig. Das Sperren von Domains und IPs ist inhärent reaktiv und daher immer ein nachgelagerter Schutz. Empfehlung: Sperrung des Zugriffs auf die Liste der aktuell aktiven URLs: https[:]//urlhaus[.]abuse[.]ch/downloads/text_online/ (wird alle 5 Minuten aktualisiert)
Wirkstelle der Maßnahme	Spam-Filter / Web-Proxy
Kann es in jeder Institution, an den Netzübergängen, für mehrere Institutionen (DL) umgesetzt werden	ja
Notwendige Voraussetzungen (System, Tool, Programm, Produkt, ...)	Einsatz Spam-Filter auf Mailserver / Web-Proxy
Material / Links / Hilfen / Beschreibungen wie umsetzbar	abhängig von eingesetztem Mailserver / Spam-Filter / Web-Proxy
Risiken und Nebenwirkungen, was passiert wenn umgesetzt, was geht dann wahrscheinlich nicht mehr	Die URLs führen zu kompromittierten Websites. Bei einer Sperrung des Zugriffs auf den Hostnamen können auch legitime Inhalte der kompromittierten Website nicht mehr abgerufen werden. Dienstlich notwendige Websites sollten davon jedoch üblicherweise nicht betroffen sein.

Bundesamt
für Sicherheit in der
Informationstechnik

VIII. Sperrung des Zugriffs auf bekannte Emotet/Trickbot C&C-Server

Schulnote Wirksamkeit	2
Schulnote Umsetzbarkeit	2
Schulnote Zeitaufwand	2
Schulnote Risiken	2
Maßnahmentitel	Sperrung des Zugriffs auf bekannte Emotet/Trickbot C&C-Server
Maßnahmenbeschreibung	Der FeodoTracker (https://feodotracker.abuse.ch) stellt IP-Adressen bekannter Emotet und Trickbot C&C-Server bereit. Eine Sperrung des Zugriffs auf die C&C-Server an zentralen Netzübergängen (z. B. Web-Proxy/Firewall) verhindert ein Nachladen von Emotet-Schadmodulen, das Nachladen weiterer Schadprogramme wie Trickbot und Datenabfluss (u.a. ausgespähte Passwörter oder E-Mail-Kommunikation). Eine Auswertung der blockierten Zugriffe ermöglicht eine Identifikation bereits infizierter Systeme. Neue IP-Adressen müssen zeitnah in die Sperrliste übernommen werden (Empfehlung: Abgleich alle 5 Minuten).
Angriffs- / Infektionsvektor	Verhindert ein Nachladen von Emotet-Schadmodulen, das Nachladen weiterer Schadprogramme wie Trickbot und Datenabfluss (u.a. ausgespähte Passwörter oder E-Mail-Kommunikation)
Wirkstelle der Maßnahme	Web-Proxy/Firewall
Kann es in jeder Institution, **an den Netzübergängen,** **für mehrere Institutionen (DL) umgesetzt werden**	ja
Notwendige Voraussetzungen (System, Tool, Programm, Produkt, ...)	Einsatz Web-Proxy/Firewall
Material / Links / Hilfen / Beschreibungen wie umsetzbar	abhängig von Web-Proxy/Firewall/Netzwerkstruktur
Risiken und Nebenwirkungen, was passiert wenn umgesetzt, was geht dann wahrscheinlich nicht mehr	Bei den C&C-Servern handelt es sich um kompromittierte Systeme. Der Zugriff auf legitime Websites auf diesen kompromittierten Systemen ist nicht mehr möglich, wenn der Zugriff auf die IP-Adresse gesperrt ist. Dienstlich notwendige Websites sollten davon jedoch nicht betroffen sein.

IX. IT-Sicherheitsinfrastruktur zum Schutz vor Malware (AV)

Schulnote Wirksamkeit	2
Schulnote Umsetzbarkeit	2
Schulnote Zeitaufwand	2
Schulnote Risiken	1
Maßnahmentitel	Software zum Schutz vor Malware (AV)
Maßnahmenbeschreibung	Bei der Auswertung von Vorfällen hat sich gezeigt, dass die optimale Konfiguration von AV-Programmen ein wesentlicher Erfolgsfaktor bei der Abwehr neuer Bedrohungen ist. Folgende Hinweise sollten unbedingt beachtet werden: • Es ist essentiell, immer die neueste Version der AV-Software einzusetzen und regelmäßig zu überprüfen, ob diese tatsächlich aktiv und wie gewünscht konfiguriert ist. („Neu“ bezieht sich ausdrücklich auf die Software und nicht nur auf die Signaturen.) • Es sollten nach Möglichkeit alle verfügbaren AV-Module verwendet werden. Ein Hauptgrund für Vorfälle ist die Nichtnutzung bestimmter Module aus Datenschutzgründen oder aus Angst vor Fehlalarmen. Als besonders wichtig haben sich Verfahren auf Basis verhaltensbasierter Analysen (inkl. KI und Machine Learning), Sandbox-Analysen und virtuelles Patchen erwiesen. • Ein modernes AV-Portfolio besteht aus einer Vielzahl von Produkten für unterschiedliche Einsatzzwecke. Bei der Produktauswahl sollten Experten mitwirken, die die Produkte sehr gut kennen. So ist es z. B. ein häufiger Fehler, auf Servern ein Schutzprodukt für Clients zu installieren, dem wichtige Module fehlen. • Ein wesentlicher Baustein der IT-Sicherheitsinfrastruktur ist ein effizientes Schwachstellenmanagement. • Die Logs der AV-Produkte müssen unbedingt regelmäßig (bei Vorfällen auch rückwirkend) auf Auffälligkeiten hin geprüft werden. • Bei der Auswahl von Produkten und der Konfiguration sollte die Hilfe von fachkundigen Experten in Anspruch genommen werden. Auch die Funktionsweise und Konfiguration aller IT-Sicherheitsprodukte sollten regelmäßig überprüft werden. Insbesondere nach Funktionsupdates müssen sich die Administratoren mit neuen oder veränderte Funktionen und Einstellungen vertraut machen. • Alle Abläufe bei der Behandlung von Vorfällen müssen vor dem ersten Vorfall festgelegt sein. Beispielsweise muss geklärt werden, auf welche Support- und Serviceleistungen und Dienstleister zurückgegriffen werden kann, wie z. B. kurzfristig Hilfe vor Ort

	organisiert werden kann. Dabei muss auch durchgespielt werden, wie mit externen Support und Servicemitarbeitern zusammengearbeitet werden kann: Welche Informationen braucht der Support? Welche Support-Tools sind notwendig? Welche Daten kommen dabei möglicherweise in fremde Hände? Wie kann ein Fernzugriff ermöglicht werden? Insbesondere müssen alle betroffenen Organisationseinheiten (z. B. Datenschutz, CISO, Personalvertretung, Geheimschutz) vorher informiert und beteiligt werden, damit im Notfall nicht wertvolle Zeit durch das Einholen von Genehmigungen verloren wird.
Angriffs- / Infektionsvektor	alle
Wirkstelle der Maßnahme	diverse
Kann es in jeder Institution, an den Netzübergängen, für mehrere Institutionen (DL) umgesetzt werden	ja ja ja
Notwendige Voraussetzungen (System, Tool, Programm, Produkt, ...)	AV-Software, Schulungsmaßnahmen, Servicevertrag

Bundesamt
für Sicherheit in der
Informationstechnik

X. Sichere Konfiguration von Microsoft-Office-Produkten

Schulnote Wirksamkeit	1
Schulnote Umsetzbarkeit	3
Schulnote Zeitaufwand	3
Schulnote Risiken	3
Maßnahmentitel	Sichere Konfiguration von Microsoft-Office-Produkten
Maßnahmenbeschreibung	Umsetzung der BSI-Empfehlungen zur sicheren Konfiguration von Microsoft-Office-Produkten
Angriffs- / Infektionsvektor	Microsoft-Office-Dokumente, Microsoft-Outlook-E-Mails
Wirkstelle der Maßnahme	Unsignierte Makros werden nicht ausgeführt, Links werden nicht mehr automatisch verfolgt, E-Mails werden als Plain-Text angezeigt.
Kann es in jeder Institution, an den Netzübergängen, für mehrere Institutionen (DL) umgesetzt werden	Ja nein nein
Notwendige Voraussetzungen (System, Tool, Programm, Produkt, ...)	keine
Material / Links / Hilfen / Beschreibungen wie umsetzbar	https[:]//www[.]allianz-fuer-cybersicherheit[.]de/ACS/DE/_/downloads/BSI-CS/BSI-CS_135[.]html https[:]//www[.]allianz-fuer-cybersicherheit[.]de/ACS/DE/_/downloads/BSI-CS/BSI-CS_140[.]html https[:]//www[.]allianz-fuer-cybersicherheit[.]de/ACS/DE/_/downloads/BSI-CS/BSI-CS_136[.]htm https[:]//www[.]allianz-fuer-cybersicherheit[.]de/ACS/DE/_/downloads/BSI-CS/BSI-CS_139[.]html https[:]//www[.]allianz-fuer-cybersicherheit[.]de/ACS/DE/_/downloads/BSI-CS/BSI-CS_137[.]html https[:]//www[.]allianz-fuer-cybersicherheit[.]de/ACS/DE/_/downloads/BSI-CS/BSI-CS_141[.]html https[:]//www[.]allianz-fuer-cybersicherheit[.]de/ACS/DE/_/downloads/BSI-CS/BSI-CS_138[.]html Microsoft-Dokumentation
Risiken und Nebenwirkungen, was passiert wenn umgesetzt, was geht dann wahrscheinlich nicht mehr	u.a. werden nicht-signierte Makros nicht mehr ausgeführt

Bundesamt
für Sicherheit in der
Informationstechnik

XI. Deaktivierung von unsignierten Macros und in MS Office (Word, Excel, Powerpoint) mittels Gruppenrichtlinien

Schulnote Wirksamkeit	1*
Schulnote Umsetzbarkeit	3
Schulnote Zeitaufwand	6
Schulnote Risiken	3
Maßnahmentitel	Deaktivierung von unsignierten Macros und in MS Office (Word, Excel, Powerpoint) mittels Gruppenrichtlinien
Maßnahmenbeschreibung	Aktivierung einer Gruppenrichtlinie, um unsignierte Macros zu verbieten: https[:]//www[.]windowspro[.]de/wolfgang-sommergut/makros-office-2016-2019-einschraenken-blockieren-gruppenrichtlinien Benötigt ein adäquates Zertifikatsmanagement.
Angriffs- / Infektionsvektor	Erstinfektion über Ausführung von Macros in Office-Dokumenten. Dabei ist unerheblich über welchen Weg (Mail mit Dateianlage oder Mail mit Link) diese Office-Dokumente übertragen werden. Eine Sekundärinfektion durch Nachladen weiterer Schadsoftware über HTTP/HTTPS wie beispielsweise Trickbot und Ryuk wird durch diese Maßnahme NICHT verhindert.
Wirkstelle der Maßnahme	Verhinderung unsignierter Macros in MS Office.
Kann es in jeder Institution, an den Netzübergängen, für mehrere Institutionen (DL) umgesetzt werden	ja
Notwendige Voraussetzungen (System, Tool, Programm, Produkt, ...)	Einsatz von Gruppenrichtlinien. Sollte Standard in Unternehmen sein.
Material / Links / Hilfen / Beschreibungen wie umsetzbar	https[:]//www[.]heise[.]de/security/meldung/Erpressungs-Trojaner-fernhalten-Mit-Windows-Bordmittel-Makros-in-Office-2016-global-verbieten-3149377[.]html https[:]//blogs[.]technet[.]microsoft[.]com/mmpc/2016/03/22/new-feature-in-office-2016-can-block-macros-and-help-prevent-infection/?platform=hootsuite?source=mmpc https://www.microsoft.com/en-us/download/details.aspx?id=49030 https[:]//www[.]allianz-fuer-cybersicherheit[.]de/ACS/DE/_/downloads/BSI-CS/BSI-CS_135[.]html (fortlaufend bis CS_141.html)
Risiken und Nebenwirkungen, was passiert wenn umgesetzt, was geht dann wahrscheinlich nicht mehr	Nutzung von unsignierten Macros nicht mehr möglich Schadhafte signierte Macros, deren Signatur vertraut wird, können weiterhin ausgeführt werden.

Bundesamt
für Sicherheit in der
Informationstechnik

XII. Endpoint Detection & Response

Schulnote Wirksamkeit	1
Schulnote Umsetzbarkeit	4
Schulnote Zeitaufwand	2
Schulnote Risiken	3
Maßnahmentitel	Endpoint Detection & Response
Maßnahmenbeschreibung	Moderne IT-Angriffe wie u.a. auch Emotet, investieren sehr viel Aufwand in die Umgehung etablierter IT-Sicherheitsmaßnahmen (wie Spam-Erkennung, dateiorientierte Anti-Virus Software). U.a. wird der Angriffscode permanent verändert und bereits auf den Zielsystemen vorhandene Software für Angriffe missbraucht (sog. "Living off the Land" bzw. durch Ausnutzung von .NET Fähigkeiten "Bring Your Own Land"). Dieser wiederum schleust dann die eigentliche Schadsoftware an den Erkennungssystemen vorbei. Mit IT-Sicherheitsverfahren auf Basis von dateibasierten Signaturen oder meistens nicht sehr striktem Applikations-Whitelisting sind daher einige Angriffe nicht rechtzeitig zu erkennen. Neue Verfahren, die unter verschiedenen Namen wie "Next Generation Endpoint Detection" oder "Enterprise Detection and Reaction (EDR)" angeboten werden, gehen einen anderen Weg und werden in vielen Unternehmen inzwischen mit Erfolg eingesetzt. Sie arbeiten auf Basis von IoCs auf der Ebene von sog. "Tactics, Techniques & Procedures". Bösartige Aktivitäten werden abstrakt beschrieben, indem die Abfolge oder Kombination bestimmter Aktivitäten betrachtet wird. Dabei liegt der Fokus beispielsweise auf der Inter-Prozesskommunikation und weniger auf der Beobachtung eines einzelnen Prozesses oder der Analyse einer Datei. Beispiel: Es ist hochverdächtig, wenn ein Autostart-Eintrag angelegt, PowerShell gestartet und dann mehrere Dateien verschlüsselt werden - unabhängig, welche Anwendung diese Aktionen durchgeführt hat. Manche EDR-Lösungen zeichnen wichtige Aktionen eines IT-Systems auf, um spätere forensische Analysen auf diesen Daten zu ermöglichen. Andere Lösungen bieten umfassende Möglichkeiten, um forensische Analyse auf den IT-Systemen selbst durchzuführen. Ebenso wird oft auch die Möglichkeit geboten, Prozesse für bestimmtes erkanntes Verhalten aktiv zu blocken und IT-Systeme zu isolieren. Eine empfehlenswerte EDR-Lösung zeichnet sich durch folgende Eigenschaften aus: • Monitoring und Aufzeichnung des Verhaltens von Endgeräten • Detektion von verdächtigem oder anormalem Verhalten

	• Alarmierung • Bereitstellung und Aufbereitung forensischer Details zur Analyse von Vorfällen • Unterstützung von IT-Sicherheitsverantwortlichen durch Bereitstellung von Threat Intelligence und Hinweisen zur Beseitigung von Infektionen • Aktive Reaktion auf bösartiges Verhalten eines Endgerätes zur Eindämmung der Infektion (z. B. Blocken von Prozessen, Quarantäne für verdächtige Dateien, Isolation des Endgeräts im Netzwerk) EDR-Lösungen verwenden dazu beispielsweise die folgenden Methoden: • Monitoring von Prozessen • Erkennung typischer Abfolgen von Prozessen/Aktionen, die in ihrer Kombination auf verdächtige Aktionen hindeuten • Detektion von Kommunikation mit potentiell verdächtigen Hosts • Detektion der Ausbreitung von Infektionen im Netzwerk (Lateral Movement) • Detektion von Änderungen am Dateisystem und der Registry Alle bekannten AV-Hersteller haben inzwischen EDR-Lösungen im Programm, die mit anderen Produkten aus dem Portfolio interagieren und zusammenwirken können. Es gibt auch Hersteller, die sich auf EDR-Funktionalitäten spezialisiert haben. Diese Lösungen stellen Schnittstellen zu bekannten IT-Sicherheitsprodukten (wie Endpoint-Protection, Sandox-Analyse, Firewalls) bereit, um sich in eine typische IT-Landschaft zu integrieren. Gleichzeitig ist jedoch auch Vorsicht geboten, da viele EDR Lösungen nur vorgeblich die zuvor beschrieben Detektionsverfahren umsetzen. Daher sollten grundsätzlich nur evaluierte EDR Lösungen in Betracht gezogen werden, um die zum Teil sehr hohen Risiken (s.u.) zu rechtfertigen. Da EDR Tools aufgrund ihrer Funktionsweise alle Datei- und Prozesshashes sowie auch Kommunikation zu IPs und Domains eines IT-Systems erheben, erfolgt auch eine Prüfung gegen diese IoCs.
Angriffs- / Infektionsvektor	Ausführung der ersten Stufe von Emotet / später nachgeladene Schadsoftware
Wirkstelle der Maßnahme	IT-System

Kann es in jeder Institution, an den Netzübergängen, für mehrere Institutionen (DL) umgesetzt werden	ja (bei Cloud Nutzung) nein ja
Notwendige Voraussetzungen (System, Tool, Programm, Produkt, ...)	Lizenzen der entsprechenden Software Ist bereits die Software eines AV Herstellers im Einsatz, ist häufig eine entsprechend teurere Lizenz für die EDR-Funktionalität erforderlich. Sofern keine Cloud-Lösung genutzt werden soll (siehe Risiken), ist entsprechende Hardware für die zentralen Komponenten der Software erforderlich.
Material / Links / Hilfen / Beschreibungen wie umsetzbar	MITRE ATT&CK Evaluations (https[:]//attackevals[.]mitre[.]org/): Evaluierungen verschiedener Produkte in der Kategorie EDR. ix 12/2019, Seite 84 "Next Generation Endpoint Security": Beschreibt verschiedene Produkte der u.a. Kategorie EDR und liefert eine gute Übersicht. Living off the Land: https[:]//www[.]symantec[.]com/content/dam/symantec/docs/security-center/white-papers/istr-living-off-the-land-and-fileless-attack-techniques-en[.]pdf Bring your own Land: https[:]//www[.]fireeye[.]com/blog/threat-research/2018/06/bring-your-own-land-novel-red-teaming-technique[.]html Erläuterung des IoC-Konzeptes: http[:]//detect-respond[.]blogspot[.]com/2013/03/the-pyramid-of-pain[.]html Mindeststandard Protokollierung und Detektion (https[:]//www[.]bsi[.]bund[.]de/SharedDocs/Downloads/DE/BSI/Mindeststandards/Mindeststandard_BSI_Protokollierung_und_Detektion_Version_1_0[.]pdf), Seite 12, PD 2.3.04.
Risiken und Nebenwirkungen, was passiert wenn umgesetzt, was geht dann wahrscheinlich nicht mehr	Hinsichtlich der False/Positive Rate gibt es keine zu erwartenden Einschränkungen. Während auch bei AV Software immer häufiger Cloud-Angebote benutzt werden, z.B. Reputationsdienste, benötigen die meisten EDR Tools eine zentrale Softwareplattform, in der die Informationen gesammelt und korreliert werden, welche in diesem Fall sehr viele Interne Informationen über das jeweilige Unternehmen / die Institution enthalten (bis hin zu Dateinamen von Office-Dokumenten oder Meta-Informationen über die eingesetzte Software). Aufgrund der Funktionsweise der Response Funktionalitäten kann über die zentrale Plattform

auch vollständiger Zugriff auf die IT-Systeme erlangt werden. Für eine einfache Bereitstellung bieten viele Hersteller eine Cloud-Plattform an.

Vor einem Einsatz müssen daher folgende Fragen abgewogen werden, welche dem Grunde nach für den Einsatz aller Cloud-Plattformen gelten (siehe auch Mindeststandard des BSI zur Nutzung externer Cloud Dienste) https[:]//www[.]bsi[.]bund[.]de/SharedDocs/Downloads/DE/BSI/Mindeststandards/Mindeststandard_Nutzung_externer_Cloud-Dienste[.]pdf):

- Dürfen die Daten gem. DSGVO verarbeitet werden, und welche Randbedingungen sind an die Cloud zu stellen, z.B. Speicherung der Daten in der EU?
- Ist der Betriebs- oder Personalrat zu beteiligen?
- Werden auf den IT-Systemen Daten verarbeitet, die Geschäftsgeheimnisse beinhalten und daher auch die EDR Hersteller nicht zur Kenntnis gelangen dürfen?
- Wie gut ist die Plattform in der Cloud gegen unberechtigten Zugriff durch Dritte abgesichert?
- Was passiert mit den Cloud-Daten wenn der Hersteller gewechselt werden soll?
- Darf der Hersteller der Cloud-Lösung darüber informiert sein, dass im jeweiligen Unternehmens / Institutionsnetz ein ggf. großflächiger Angriff stattfindet?
- Ist ggf. eine zusätzliches Non-Disclosure Agreement zu schließen oder eine Sicherheitsüberprüfung durchzuführen?

Erscheinen die Risiken der Cloud Lösung zu hoch, dann bieten manche Hersteller sog. On-Premise Lösungen an, welche jedoch Hardware und teilweise auch zusätzliche Softwarelizenzen für den Hypervisor erfordern.

Soll der eigentliche Mehrwert von EDR Tools genutzt werden, erfordern die Daten grundsätzlich die Begutachtung von Sicherheits-Analysten. Diese Dienstleistung kann entweder selbst erbracht werden, durch den Hersteller oder einen vertrauenswürdigen weiteren Dienstleister. Dieser Service ist jedoch im Preis der Lizenzen nicht enthalten.

Bundesamt
für Sicherheit in der
Informationstechnik

XIII. Umschreibung URLs

Schulnote Wirksamkeit	1
Schulnote Umsetzbarkeit	3
Schulnote Zeitaufwand	6
Schulnote Risiken	3
Maßnahmentitel	Umschreibung URLs
Maßnahmenbeschreibung	Nachlade-URLs werden umgeschrieben, entfernt
Kann es in jeder Institution, an den Netzübergängen, für mehrere Institutionen (DL) umgesetzt werden	am Netzübergang vom Internet zum Netz der Institution
Notwendige Voraussetzungen (System, Tool, Programm, Produkt, ...)	Voraussetzung ist eine Mailsoftware, die nativ eine Umschreibung von URLs unterstützt. Andernfalls muss eine ggf. aufwändige Anpassung durch den Anbieter erfolgen
Material / Links / Hilfen / Beschreibungen wie umsetzbar	
Risiken und Nebenwirkungen, was passiert wenn umgesetzt, was geht dann wahrscheinlich nicht mehr	Nutzer können keinen Links mehr in E-Mails aus dem Internet folgen. Je nach Art der Veränderung kann ein Nutzer den Originallink wiederherstellen. Mögliche Signaturen (S/MIME, PGP) werden durch die Veränderungen ungültig und die Mails werden im Client als Risiko eingestuft.

XIV. Mailfilterungen - Keine Office-Dokumenten die Macros und OLE enthalten zulassen

Schulnote Wirksamkeit	2
Schulnote Umsetzbarkeit	4
Schulnote Zeitaufwand	4
Schulnote Risiken	2
Maßnahmentitel	Mailfilterungen - Keine Office-Dokumenten die Macros und OLE enthalten zulassen
Maßnahmenbeschreibung	Aus dem Internet eingehende Mails sollen an einem zentralen Mailgateway gefiltert werden. Dabei sollen Dateianlagen, die Macros und OLE in Office-Dokumenten enthalten aus den E-Mails entfernt werden oder die Mails abgewiesen werden. Absender und Empfänger können entsprechend informiert werden.
Angriffs- / Infektionsvektor	Erstinfektion per E-Mail über infizierte Office-Dokumente, die als Dateianlage übertragen werden. Hilft nicht gegen Link in E-Mail, die auf infizierte Dateien verweisen. Hilft nicht gegen Sekundärinfektion durch Nachladen weiterer Schadsoftware über HTTP/HTTPS wie beispielsweise Trickbot und Ryuk.
Wirkstelle der Maßnahme	Mailgateway
Kann es in jeder Institution, **an den Netzübergängen,** **für mehrere Institutionen (DL) umgesetzt werden**	ja
Notwendige Voraussetzungen (System, Tool, Programm, Produkt, ...)	Beschaffung eines entsprechenden Filtersystems
Material / Links / Hilfen / Beschreibungen wie umsetzbar	
Risiken und Nebenwirkungen, was passiert wenn umgesetzt, was geht dann wahrscheinlich nicht mehr	Office-Dokumente mit Macros werden zurückgewiesen bzw. gefiltert. Absender und Empfänger kann informiert werden.

Bundesamt
für Sicherheit in der
Informationstechnik

XV. Notfallmaßnahme: Verbot der privaten Nutzung des Internets

Schulnote Wirksamkeit	4
Schulnote Umsetzbarkeit	1
Schulnote Zeitaufwand	1
Schulnote Risiken	4
Maßnahmentitel	Verbot der privaten Nutzung des Internets
Maßnahmenbeschreibung	Verbot der privaten Nutzung des Internets durch Dienstanweisung. Sensibilisierung der Nutzer. Sofern die private Nutzung des Internets für private Zwecke erlaubt ist, besteht die Gefahr, dass darüber eine Erstinfektion erfolgt. Im Fall der Nutzung von Webmail wird in der Regel die E-Mail ohne weitere Prüfung inkl. Dateianlagen und Links bereitgestellt. Lädt ein Anwender so eine infizierte Office-Datei und aktiviert die Macroausführung, kann eine Erstinfektion erfolgen. Neben E-Mail werden Dateien oder Links auch über andere Internet-Dienste bereitgestellt werden. Das Hauptziel dieser Maßnahme besteht darin, die Anzahl an E-Mails, welche geöffnet werden, zu verringern. Erleichterung der Reaktion durch vereinfachte rechtliche Rahmenbedingungen z.B. zur Logdaten-Auswertung und Sperrung.
Angriffs- / Infektionsvektor	Herunterladen von infizierten Dateien.
Wirkstelle der Maßnahme	Organisatorisch
Kann es in jeder Institution, **an den Netzübergängen,** **für mehrere Institutionen (DL) umgesetzt werden**	ja
Notwendige Voraussetzungen (System, Tool, Programm, Produkt, ...)	keine
Material / Links / Hilfen / Beschreibungen wie umsetzbar	
Risiken und Nebenwirkungen, was passiert wenn umgesetzt, was geht dann wahrscheinlich nicht mehr	Demotivierung der Mitarbeiter

Bundesamt
für Sicherheit in der
Informationstechnik

XVI. Automatische Analyse und Bewertung von E-Mails durch ein Sandbox-Analyse-System

Schulnote Wirksamkeit	2
Schulnote Umsetzbarkeit	3
Schulnote Zeitaufwand	2
Schulnote Risiken	2
Maßnahmentitel	Automatische Analyse und Bewertung von E-Mails durch ein Sandbox-Analyse-System
Maßnahmenbeschreibung	Es besteht die Möglichkeit, E-Mail-Anhänge und Links in E-Mails zusätzlich neben bestehenden Sicherheitsmaßnahmen automatisch durch ein Sandbox-Analyse-System analysieren und bewerten zu lassen bevor E-Mails an den Empfänger zugestellt werden. Die Nutzung des Sandbox-Analyse-Systems ist dabei nicht auf die Untersuchung von E-Mails beschränkt. Es kann ebenso für die Detektion von Schadsoftware in beliebigen Dateien verwendet werden.
Angriffs- / Infektionsvektor	Schadsoftware in E-Mail-Anhängen und Links auf bösartige Web-Seiten
Wirkstelle der Maßnahme	SMTP-Server
Kann es in jeder Institution, an den Netzübergängen, für mehrere Institutionen (DL) umgesetzt werden	ja, ja, ja
Notwendige Voraussetzungen (System, Tool, Programm, Produkt, ...)	Für die Bearbeitung von Alarmen muss ein geeigneter Prozess eingerichtet werden. Die Analyse der Alarme erfordert entsprechend ausgebildetes Personal mit ausreichenden Ressourcen.
Risiken und Nebenwirkungen, was passiert wenn umgesetzt, was geht dann wahrscheinlich nicht mehr	Je nach Analysezeit und Auslastung des Sandbox-Systems kann es zu Verzögerungen bei der E-Mail-Zustellung kommen. Falls eine Datei oder eine URL als schadhaft klassifiziert wird, können u. U. Daten (z. B. Datei, Dateiname, Betreff einer E-Mail) an den Hersteller der Sandbox-Analyse-Lösung übertragen werden. Welche Daten übertragen werden, ist konfigurationsabhängig und variiert von Hersteller zu Hersteller. Bei der Produktauswahl sollten daher umfangreiche Informationen über die Lösung eingeholt werden (auch um den Anforderungen der DSGVO gerecht zu werden).

Bundesamt
für Sicherheit in der
Informationstechnik

XVII. Einsatz von Produkten, die auf Ungereimtheiten in E-Mails hinweisen

Schulnote Wirksamkeit	3
Schulnote Umsetzbarkeit	2
Schulnote Zeitaufwand	4
Schulnote Risiken	1
Maßnahmentitel	Einsatz von Produkten, die auf Ungereimtheiten in E-Mails hinweisen
Maßnahmenbeschreibung	Es besteht die Möglichkeit, in E-Mail-Clients auf Ungereimtheiten in E-Mails hinzuweisen. Beispielsweise könnte ein Warnhinweis angezeigt werden wenn sich der tatsächliche Absender vom angezeigten Absender unterscheidet oder wenn eine E-Mail von einem internen Absender von einem externen SMTP-Server geschickt wird.
Angriffs- / Infektionsvektor	Phishing E-Mails
Wirkstelle der Maßnahme	E-Mail-Programm und SMTP-Server
Kann es in jeder Institution, an den Netzübergängen, für mehrere Institutionen (DL) umgesetzt werden	ja, teilweise, ja
Notwendige Voraussetzungen (System, Tool, Programm, Produkt, ...)	
Risiken und Nebenwirkungen, was passiert wenn umgesetzt, was geht dann wahrscheinlich nicht mehr	Es kann zu Fehlalarmen (z. B. bei Newslettern) kommen. Auch kann weiterhin versehentliches oder absichtliches Anklicken durch den Nutzer nicht verhindert werden.

Bundesamt
für Sicherheit in der
Informationstechnik

XVIII. Gekapseltes Surfen im Internet und sicherer Umgang mit Dateidownloads und E-Mail-Anhängen

Schulnote Wirksamkeit	1
Schulnote Umsetzbarkeit	3
Schulnote Zeitaufwand	2
Schulnote Risiken	2
Maßnahmentitel	Gekapseltes Surfen im Internet und sicherer Umgang mit Dateidownloads und E-Mail-Anhängen
Maßnahmenbeschreibung	Es gibt IT-Sicherheitsprodukte, die es ermöglichen, Web-Browser, E-Mail-Anhänge und Dateidownloads gekapselt auszuführen. Dies kann beispielsweise lokal auf einem Arbeitsplatzrechner in einer virtuellen Maschine oder über eine zentrale ReCoBS-Lösung innerhalb einer DMZ erfolgen. Je nach Produkt können Dateidownloads und E-Mail-Anhänge nicht nur gekapselt betrachtet, sondern ebenfalls sicher bearbeitet werden.
Angriffs- / Infektionsvektor	Schwachstellen im Web-Browser und Schadprogramme in Dateidownloads sowie E-Mail-Anhängen
Wirkstelle der Maßnahme	Web-Browser und E-Mail-Client
Kann es in jeder Institution, an den Netzübergängen, für mehrere Institutionen (DL) umgesetzt werden	ja, nein, ja
Notwendige Voraussetzungen (System, Tool, Programm, Produkt, ...)	IT-Sicherheitsprodukt Da jedes Produkt unterschiedliche Stärken und Schwächen aufweist, muss immer eine individuelle Bewertung durch die Bereiche IT-Betrieb und Informationssicherheit vorgenommen werden.
Material / Links / Hilfen / Beschreibungen wie umsetzbar	
Risiken und Nebenwirkungen, was passiert wenn umgesetzt, was geht dann wahrscheinlich nicht mehr	Entsprechende Lösungen bieten typischerweise nicht die gleiche Performance und den gleichen Komfort wie ein Standard-Arbeitsplatz mit Windows oder Linux.

Bundesamt
für Sicherheit in der
Informationstechnik

XIX. Maßnahmen gegen Social Engineering

Schulnote Wirksamkeit	3
Schulnote Umsetzbarkeit	3
Schulnote Zeitaufwand	2
Schulnote Risiken	1
Maßnahmentitel	Maßnahmen gegen Social Engineering
Maßnahmenbeschreibung	Fast alle IT-Angriffe haben eine Social Engineering-Komponente, mit der ein IT-Nutzer dazu gebracht werden soll, einen Anhang zu öffnen, auf einen Link zu klicken oder eine Aktion (z. B. Ausführung eines Makros, Installation eines Browser Add-ons) freizugeben. Die Täuschung der IT-Nutzer ist gerade bei den aktuellen Emotet-Angriffen sehr gut gemacht - perfekt ist sie aber nicht, sodass aufmerksame, gut geschulte IT-Anwender einige Täuschungsversuche durchaus erkennen können. Allgemeine Warnhinweise im Intranet ("Aus gegebenem Anlass weisen wir darauf hin, ...") oder die Drohung mit Dienstanweisungen haben sich in der Praxis allerdings als unwirksam erwiesen. Viele Unternehmen haben hingegen sehr gute Erfahrungen mit professionellen Sensibilisierungsmaßnahmen gemacht. Dabei konnten die folgenden Erfolgsfaktoren identifiziert werden: • IT-Nutzer sind der wichtigste Teil einer Sicherheitsarchitektur und sollten als Partner der IT verstanden werden. Mitarbeiter, die sich mit ihrem Arbeitgeber identifizieren und Verantwortung haben, sind erfahrungsgemäß gerne bereit, an Sicherheitsmaßnahmen mitzuwirken. Sicherheitsmaßnahmen, die nicht verstanden oder als Schikane empfunden werden, werden dagegen häufig umgangen. Dazu gehört auch, dass IT-Nutzern eine IT-Umgebung zur Verfügung gestellt wird, die ihnen die einfache Erledigung ihrer Aufgaben ermöglicht. Bewusste Einschränkungen in Komfort und Funktion sollten immer erklärt werden. • IT-Nutzer sollten sehr konkret und praxisnah sensibilisiert werden. Echte Vorfälle sollten auf keinen Fall verschwiegen, sondern als Beispiel verwendet werden, um andere zu warnen. Dabei ist es unerlässlich, die Mitarbeiter ins Vertrauen zu ziehen. Auch über abgewehrte Angriffe kann als positives Beispiel berichtet werden. • Es sollte mit professionellen Dienstleistern zusammengearbeitet werden. • Konkrete, interaktive Schulungen zur Erkennung von Angriffen sind wesentlich effektiver als passive

	Informationen durch Intranethinweise oder Flyer. Innerhalb professioneller Schulungen werden echte Angriffe besprochen, Rollenspiele durchgeführt, erklärt, wie die Echtheit einer E-Mail mit Hilfe des Headers überprüft werden kann und welche Möglichkeiten es gibt, Links in E-Mails zu verschleiern. Wenn bei den Schulungen ein Bezug zur privaten IT-Nutzung hergestellt wird, steigert dies Aufmerksamkeit und Nutzwert erheblich. • Die Durchführung lebensnaher Social Engineering-Angriffe, hält Mitarbeiter in Alarmbereitschaft und erzielt die besten Lerneffekte. Beispiele: Versand von Fake-Mails mit manipulierten Anhängen, Durchführung von Testanrufen, Verteilung präparierter USB-Sticks • Mit allen Maßnahmen sollten positive Anreize gesetzt werden (z. B. Belohnung, wenn ein Mitarbeiter einen Testangriff erkannt hat). Bei grober Fahrlässigkeit oder der bewussten Umgehung von Sicherheitsmaßnahmen müssen aber ebenfalls konsequente Maßnahmen gegen Mitarbeiter eingeleitet werden. • Das Incident Response Team muss so aufgebaut werden, dass es auf eine steigende Zahl von Verdachtsmeldungen reagieren kann. Meldungen müssen immer ernst genommen werden, um Mitarbeiter nicht zu demotivieren. • IT-Nutzer sollten nach Möglichkeit mit technischen Maßnahmen bei der Erkennung von Angriffen unterstützt werden, z. B.: Hinweise auf verdächtige E-Mail-Header anzeigen, Tools zur Anzeige des E-Mail-Headers zur Verfügung stellen, Fake-Adressen automatisiert erkennen, Maßnahmen zum Schutz vor Makros umsetzen, Makros nur einsetzen, wenn sie unbedingt erforderlich sind. Aufgrund des sehr gut gemachten Verteilmechanismus von Emotet-SPAM mittels den Empfängern bekanntem Absender und Inhalt in der Mail ist diese Maßnahme jedoch nicht so erfolgsversprechend wie sonst üblich.
Angriffs- / Infektionsvektor	E-Mail
Wirkstelle der Maßnahme	IT-Nutzer
Notwendige Voraussetzungen (System, Tool, Programm, Produkt, ...)	Vertrag mit einem qualifizierten Dienstleister
Risiken und Nebenwirkungen, was passiert wenn umgesetzt, was geht dann wahrscheinlich nicht mehr	keine technischen Einschränkungen, ggf. besonderes Misstrauen der Nutzer mit häufigeren Kontakten zum IT-Support

Bundesamt
für Sicherheit in der
Informationstechnik

XX. Entkoppelung des Betriebssystems vom Internet

Schulnote Wirksamkeit	1 (Unterbindung C&C Kommunikation und Downloader)
Schulnote Umsetzbarkeit	2
Schulnote Zeitaufwand	4
Schulnote Risiken	2
Maßnahmentitel	Entkopplung des Betriebssystems vom Internet
Maßnahmenbeschreibung	Das Betriebssystem wird vom Internet entkoppelt. Anwendungen, die einen Internetzugang erfordern, dürfen ausschließlich über einen Proxy-Server mit Whitelist an das Internet angebunden werden. Lokal installierte Webbrowser sollten nur Zugriff auf das lokale Intranet erhalten. Für den Aufruf von Webseiten im Internet sollte eine gekapselte Surfumgebung verwendet werden (siehe XXI. Gekapseltes Surfen).
Angriffs- / Infektionsvektor	Schwachstellen im Betriebssystem und teilweise Schadprogramme in Dateidownloads Nachladen von Schadcode und –programmen durch Betriebssystemfunktionen oder sonstige Software, Skripten, etc.
Wirkstelle der Maßnahme	Betriebssystem
Kann es in jeder Behörde, an den IVBB Netzübergängen, für mehrere Behörden (DL) umgesetzt werden	ja nein ja
Notwendige Voraussetzungen (System, Tool, Programm, Produkt, ...)	Eigenbetrieb von Diensten, wie bspw. Windows-Update, Zeitserver, Zertifikatssperrlisten, Namensauflösung (DNS), etc.
Material / Links / Hilfen	
Risiken und Nebenwirkungen, was passiert wenn umgesetzt, was geht dann wahrscheinlich nicht mehr	Betriebssystemfunktionen, die auf das Internet angewiesen sind (bei Windows 10 bspw. u.a. die integrierte Windows-Hilfe) sind nicht mehr über das Betriebssystem abrufbar. Anwendungen können nicht mehr beliebig auf das Internet zugreifen, hierdurch können bestimmte Inhalte nicht mehr zur Verfügung stehen.

Bundesamt
für Sicherheit in der
Informationstechnik

XXI. Netzsegmentierung: Unterbindung Client-zu-Client Kommunikation („Direktverbindungen“)

Schulnote Wirksamkeit	3
Schulnote Umsetzbarkeit	2
Schulnote Zeitaufwand	3
Schulnote Risiken	2
Maßnahmentitel	Netzsegmentierung: Unterbindung direkter Client-zu-Client Kommunikation, Netzwerkisolation von Endsystemen
Maßnahmenbeschreibung	Eine direkte Client-zu-Client Kommunikation wird unterbunden und nur notwendige Kommunikation zwischen Client und Serverdiensten zugelassen (Einschränkung der Kommunikationsbeziehungen). Hierdurch soll eine laterale Ausbreitung von Schadsoftware im Netzwerk unterbunden werden.
Angriffs- / Infektionsvektor	Schwachstellen im Betriebssystem und Diensten, Verbreitung von Schadsoftware im lokalen Netzwerk (z.B. über Dateifreigaben, RPC, WMI, DCOM, PowerShell Remoting oder anderen Diensten und Protokollen.
Wirkstelle der Maßnahme	Betriebssystem
Kann es in jeder Behörde, an den IVBB Netzübergängen, für mehrere Behörden (DL) umgesetzt werden	ja nein ja
Notwendige Voraussetzungen (System, Tool, Programm, Produkt, ...)	Anpassung der Client-Schnittstellen über eine Firewallkonfiguration (z.B. lokal im Betriebssystem integrierte Firewall) Einsatz von Port Isolation auf Netzkomponenten (Anforderungen an die Netzwerkinfrastruktur)
Material / Links / Hilfen	SYS.2.1.A23 Nutzung von Client-Server-Diensten
Risiken und Nebenwirkungen, was passiert wenn umgesetzt, was geht dann wahrscheinlich nicht mehr	keine

Bundesamt
für Sicherheit in der
Informationstechnik

XXII. Einschränkung von Skriptsprachen und –umgebungen

Schulnote Wirksamkeit	2
Schulnote Umsetzbarkeit	2
Schulnote Zeitaufwand	2
Schulnote Risiken	1
Maßnahmentitel	Einschränkung von Skriptsprachen und -umgebungen
Maßnahmenbeschreibung	Skriptsprachen und –umgebungen (PowerShell, Windows Scripting Host, etc.) sollten auf Clients deaktiviert werden, wenn sie nicht benötigt werden. Grundsätzlich soll sollte die Ausführung von Skripten und Befehlen über Skriptsprachen protokolliert werden. Für die PowerShell sollte der Constrained Language Mode und ausschließlich die Ausführung signierter Skripte aktiviert sein. Hierdurch wird der zur Verfügung stehende Befehls-/Kommandoraum eingeschränkt.
Angriffs- / Infektionsvektor	Nachladen von Schadcode / Ausführung von schadhaften Befehlen über Skriptsprachen und –umgebungen, wie bspw. PowerShell, etc.
Wirkstelle der Maßnahme	Betriebssystem
Kann es in jeder Behörde, an den IVBB Netzübergängen, für mehrere Behörden (DL) umgesetzt werden	ja nein ja
Notwendige Voraussetzungen (System, Tool, Programm, Produkt, ...)	Anpassung der Client-Konfiguration (z.B. über Gruppenrichtlinie) Entfernung nicht benötigter Komponenten
Material / Links / Hilfen	SYS.2.1.A16 Deaktivierung und Deinstallation nicht benötigter Komponenten und Kennungen Windows 8.1.: SYS.2.2.2.A16 Verwendung der Windows PowerShell (CIA) Windows 10: SYS.2.2.3.A22 Windows PowerShell (CIA) PowerShell Constrained Language Mode: https[:]//devblogs.microsoft[.]com/powershell/powershell-constrained-language-mode/
Risiken und Nebenwirkungen, was passiert wenn umgesetzt, was geht dann wahrscheinlich nicht mehr	keine