Liebe MandantInnen,

das BSI warnt aktuell vor Cyberangriffen https://www.allianz-fuer-cybersicherheit.de/ACS/DE/Informationspool/Themen/Emotet/emotet_node.html

Wir haben Ihnen die **präventiven Maßnahmenempfehlung des BSI** in folgender **Checkliste** formatiert, damit Sie sich **einen schnellen Überblick über Ihren eigenen aktuellen Sicherheits-Status-Quo verschaffen** können und im **Fall der Fälle (auf Seite 4) schnell wissen, was zu tun ist**.

Folgende Maßnahmen MÜSSEN aus Sicht des BSI innerhalb der IT-Infrastruktur umgesetzt werden:	**erfüllt**
Regelmäßige Information und Sensibilisierung von Nutzern für die Gefahren durch E-Mail-Anhänge oder Links - einschließlich des Hinweises, auch bei vermeintlich bekannten Absendern (siehe auch gefälschte Absenderadressen) Dateianhänge oder Links bzw. über diese heruntergeladene Dateien im Zweifel nur nach Rücksprache mit dem Absender zu öffnen (insbesondere auch keine Office-Dokumente). Nutzer sollten Auffälligkeiten umgehend an den IT-Betrieb und den IT-Sicherheitsbeauftragten melden.	☐
Zeitnahe Installation von den Herstellern bereitgestellter Sicherheitsupdates für Betriebssysteme und Anwendungsprogramme (insbesondere Web-Browser, Browser-Plugins, E-Mail-Clients, Office-Anwendungen, PDF-Dokumentenbetrachter) – idealerweise automatisiert über eine zentrale Softwareverteilung.	☐
Einsatz zentral administrierter AV-Software. Regelmäßige Prüfung, ob Updates von AV-Signaturen erfolgreich auf allen Clients ausgerollt werden.	☐
Regelmäßige Durchführung von mehrstufigen Datensicherungen (Backups), insbesondere von Offline-Backups. Zu einem Backup gehört immer auch die Planung des Wiederanlaufs und ein Test der Rückspielung von Daten.	☐
Regelmäßiges manuelles Monitoring von Logdaten, idealerweise ergänzt um automatisiertes Monitoring mit Alarmierung bei schwerwiegenden Anomalien.	☐
Netzwerk-Segmentierung (Trennung von Client-/Server-/Domain-Controller-Netzen sowie Produktionsnetzen mit jeweils isolierter Administration) nach unterschiedlichen Vertrauenszonen, Anwendungsbereichen und/oder Regionen.	☐
Fehler interner Nutzer stellen die größte Gefahr dar. Alle Nutzerkonten dürfen daher nur über die minimal zur Aufgabenerfüllung notwendigen Berechtigungen verfügen.	☐

mb-datenschutz GmbH
Klosterstr. 34 - 35, 13581 Berlin
GF: Martina Böhmer, Gerald Böhmer
HRB Berlin-Charlottenburg 202590
Steuernummer: DE321496515

https://mb-datenschutz.de

Fon: 030 / 367 2775 - 0
Fax: 030 / 367 2775 - 99
E-Mail: info@mb-datenschutz.de

Folgende Maßnahmen SOLLTEN darüber hinaus umgesetzt sein, um eine Infektion mit Schadprogrammen und deren Ausbreitung im internen Netz zu erschweren:	**erfüllt**
Je weniger Programme zum Öffnen von unbekannten Dateien zur Verfügung stehen, desto weniger Schwachstellen und Fehlkonfigurationen können durch einen Angreifer ausgenutzt werden. Daher sollte nicht benötigte Software generell deinstalliert werden. In Web-Browsern sollten insbesondere die Ausführung aktiver Inhalte zumindest eingeschränkt (z. B. Click-to-Play oder Einschränken auf Intranetseiten) sowie nicht zwingend benötigte Browser-Plugins (z. B. Flash, Java, Silverlight) entfernt werden.	☐
Deaktivierung von Makros und OLE-Objekten in Microsoft Office, Verwendung von signierten Makros: Die generelle Ausführung von Makros sollte (zentral per Gruppenrichtlinie) deaktiviert werden. Innerhalb der Organisation verwendete Makros sollten digital signiert sein. Es sollten nur Makros mit festgelegten digitalen Signaturen von konfigurierten vertrauenswürdigen Orten zugelassen werden.	☐
Einschränkung bzw. Deaktivierung des Windows Script Hosts (WSH).	☐
Einsatz von Application-Whitelisting, z. B. mittels Microsoft AppLocker	☐
Vermeidung von statischen lokalen Administratorkennwörtern, z. B. mittels Microsoft Local Administrator Password Solution (LAPS).	☐
Deaktivierung administrativer Freigaben (Admin$, IPC$)	☐
Verwendung von Zwei-Faktor-Autorisierung zur Anmeldung an Systemen. Dies verhindert die automatisierte Ausbreitung von Schadprogrammen im Netzwerk mittels ausgespähter Zugangsdaten.	☐
Dateiendungen sollten standardmäßig angezeigt werden. Dadurch können Nutzer doppelte Dateiendungen wie bei "Rechnung.pdf.exe" einfacher erkennen.	☐
Verwendung von Plain-Text statt HTML für E-Mails. Viele E-Mails werden heutzutage im HTML-Format versendet. Damit diese im E-Mail-Client korrekt dargestellt werden können, nutzt dieser Client die gleichen Mechanismen zur Darstellung wie ein Web-Browser. E-Mail-Clients enthalten jedoch häufig Schwachstellen, welche bei Web-Browsern durch zusätzliche Sicherheitsmaßnahmen eingedämmt werden. Dieser umgebende Schutz ist bei E-Mail-Programmen in der Regel weniger ausgeprägt. Die größte Schutzwirkung bietet daher die Darstellung von E-Mails als Textdarstellung (oft als "Nur-Text" bzw. "Reiner Text" bezeichnet). Ein weiterer sicherheitstechnischer Vorteil dieser Darstellung ist, dass verschleierte URLs in der Textdarstellung leicht erkannt werden können (in einer HTML-E-Mail könnte eine als "www.bsi.de" angezeigte URL z. B. tatsächlich auf "www.schadsoftwaredownload.de" verweisen). Mindestens sollte die Ausführung aktiver Inhalte bei Verwendung von HTML-Mails unterdrückt werden.	☐

mb-datenschutz GmbH
Klosterstr. 34 - 35, 13581 Berlin
GF: Martina Böhmer, Gerald Böhmer
HRB Berlin-Charlottenburg 202590
Steuernummer: DE321496515

https://mb-datenschutz.de

Fon: 030 / 367 2775 - 0
Fax: 030 / 367 2775 - 99
E-Mail: info@mb-datenschutz.de

Angreifer fälschen häufig die Absenderangabe in E-Mails, um dem Empfänger einen bekannten (vertrauenswürdigen) internen oder externen Absender vorzutäuschen. Oft wird dabei der gefälschte Absender inkl. Mailadresse in den so genannten Anzeigenamen (Realnamen) eingetragen, während die eigentliche Absenderadresse der E-Mail einen kompromittierten und zum Versand der E-Mail missbrauchten Account enthält. E-Mail-Clients sollten daher so konfiguriert werden, dass sie nicht nur den Anzeigenamen, sondern auch die vollständige Mailadresse des Absenders anzeigen. Potenzielle Angriffsversuche sollten im E-Mail-Client entsprechend markiert oder gar nicht erst zugestellt werden.	☐
E-Mail-Server sollten von extern eingelieferte E-Mails mit Absenderadressen der eigenen Organisation (sei es im Envelope-Header, im From-Header oder im Anzeigenamen) ablehnen, in Quarantäne verschieben oder mindestens im Betreff deutlich markieren.	☐
E-Mails mit ausführbaren Dateien (.exe, .scr, .chm, .bat, .com, .msi, .jar, .cmd, .hta, .pif, .scf, etc.) im Anhang – auch in Archiven wie .zip – sollten blockiert oder in Quarantäne verschoben werden. Sollte eine generelle Filterung für manche Dateitypen oder Empfänger aufgrund von zwingend notwendigen Arbeitsabläufen nicht möglich sein, sollten entsprechende E-Mails deutlich im Betreff markiert werden.	☐
Verschlüsselung von E-Mails mittels PGP oder S/MIME, um ein Ausspähen potenziell vertraulicher E-Mail-Inhalte zu verhindern. Ein durchgängiger Einsatz von digitalen Signaturen hilft zudem bei der Validierung bekannter E-Mail-Absender. Dazu müssen die zur Verifizierung benötigten Informationen einfach erreichbar auf der Website unter Kontakten einsehbar sein.	☐
Direkte Verbindungen zwischen Clients in einem Netzwerk sollten mittels Firewall unterbunden werden (insbesondere SMB-Verbindungen, PowerShell, PsExec und RDP).	☐

mb-datenschutz GmbH
Klosterstr. 34 - 35, 13581 Berlin
GF: Martina Böhmer, Gerald Böhmer
HRB Berlin-Charlottenburg 202590
Steuernummer: DE321496515

https://mb-datenschutz.de

Fon: 030 / 367 2775 - 0
Fax: 030 / 367 2775 - 99
E-Mail: info@mb-datenschutz.de

Was ist zu tun, wenn in meiner Organisation bereits IT-Systeme infiziert sind?	erfüllt
Potenziell infizierte Systeme sollten umgehend vom Netzwerk isoliert werden, um eine weitere Ausbreitung der Schadsoftware im Netz durch Seitwärtsbewegungen (Lateral Movement) zu verhindern. Dazu das Netzwerkkabel (LAN) ziehen. Gerät **nicht** herunterfahren oder ausschalten, also insbesondere **nicht** das Netzkabel (Strom) ziehen. Gegebenenfalls forensische Sicherung inkl. Speicherabbild für spätere Analysen (durch Dienstleister oder Strafverfolgungsbehörden) erstellen.	☐
Keinesfalls darf eine Anmeldung mit privilegierten Nutzerkonten auf einem potenziell infizierten System erfolgen, während es sich noch im produktiven Netzwerk befindet.	☐
Die nachgeladenen Schadprogramme werden häufig (in den ersten Stunden nach Verbreitung) nicht von AV-Software erkannt. Die Schadprogramme nehmen teilweise tiefgreifende (sicherheitsrelevante) Änderungen am infizierten System vor, die nicht einfach rückgängig gemacht werden können. Das BSI empfiehlt daher grundsätzlich, infizierte Systeme als vollständig kompromittiert zu betrachten und neu aufzusetzen.	☐
Alle auf betroffenen Systemen (zum Beispiel im Web-Browser) gespeicherte bzw. nach der Infektion eingegebene Zugangsdaten sollten als kompromittiert betrachtet und die Passwörter geändert werden.	☐
Krisen-Kommunikation sollte **nicht** über kompromittierte interne E-Mail laufen, sondern über externe Adressen (wenn möglich verschlüsselt, z.B. mittels PGP). Sonst können Angreifer direkt erkennen, dass sie entdeckt wurden.	☐
Melden Sie den Vorfall - ggf. anonym - beim BSI. Diese Informationen sind Voraussetzung für ein klares IT-Lagebild und für eine frühzeitige Warnung potenziell später Betroffener durch das BSI von zentraler Bedeutung.	☐
Stellen Sie Strafanzeige. Wenden Sie sich dazu an die Zentrale Ansprechstelle Cybercrime (ZAC) in Ihrem Bundesland.	☐
Mitarbeiter-Kommunikation muss bedacht werden. Einerseits zur Unterrichtung über die Gründe des "Stillstands" sowie zu einer evtl. privaten Betroffenheit von Mitarbeitern, wenn die private Nutzung des Arbeitsplatzes erlaubt ist und dort Passwörter und Kontodaten etc. genutzt wurden (und wahrscheinlich abgeflossen sind) - Andererseits zur Sensibilisierung für den Neuanlauf inkl. der notwendigen Informationen.	☐
Proaktive Information von Geschäftspartnern/Kunden über den Vorfall mit Hinweis auf mögliche zukünftige Angriffsversuche per E-Mail mit Absenderadressen der betroffenen Organisation. Sharing is caring!	☐

mb-datenschutz, 25.09.2019, aktualisiert am 10.06.2020

mb-datenschutz GmbH
Klosterstr. 34 - 35, 13581 Berlin
GF: Martina Böhmer, Gerald Böhmer
HRB Berlin-Charlottenburg 202590
Steuernummer: DE321496515

https://mb-datenschutz.de

Fon: 030 / 367 2775 - 0
Fax: 030 / 367 2775 - 99
E-Mail: info@mb-datenschutz.de