18 technische Mindeststandards für 2022

(Version Kleinstunternehmen ohne Domäne)

Diese Anforderungen richten sich an Kleinstunternehmen ohne eigene Domäne und größere Heiminstallationen. Eine ähnliches Anforderungsdokument für kleine – mittlere Firmen ist auch verfügbar.

Die organisierte Kriminalität verdient mit Cyberangriffen zunehmend mehr Geld. Nahezu jeden Tag gehen neue Schadensmeldungen durch die Presse und immer mehr Unternehmen sind betroffen.

Die Autoren stehen als BSI-akkreditierte APT-Response Dienstleister nahezu täglich inmitten verschlüsselter IT-Systeme von kleinen, mittleren und großen Firmen und versuchen zu retten, was noch zu retten ist. Hier müssen wir leider konstatieren: Die Angreifer aus der organisierten Kriminalität gehen zwar systematisch und planvoll vor, sind jedoch keine erfahrenen Top-Hacker. In den allermeisten Ransomware-Fällen hat man es den Angreifern durch eine mangelnde oder fehlerhafte Implementierung von Sicherheitskonzepten unnötig einfach gemacht. Für einen Incident Response Consultant, der sich Wochenenden und Nächte um die Ohren schlägt, ist es sehr frustrierend die gleichen Fehler immer und immer wieder zu sehen.

Wenn es um die Verteidigung einer digitalen Infrastruktur geht, dann ist die Abwehr von Ransomware der absolute Mindeststandard der geleistet werden muss:

i. Phishing-Schutz

Das Einfallstor ist in nahezu allen Fällen eine gut gemachte Phishing-E-Mail. Die E-Mail basiert auf einer bestehenden E-Mail-Kommunikation eines bekannten Kontaktes mit Ihrem Unternehmen. Diese wurde von den Tätern in der Regel bei einem Ihrer Kommunikationspartner erbeutet. Die EMail sieht so echt aus, dass Ihre Benutzer das Attachment oder den Link öffnen wollen, weil Sie fest an die Rechtmäßigkeit der Kommunikation glauben. Die Infektion des Rechners geschieht häufig über die Makros eines alten Office-Formats (doc,xls,ppt). Der enthaltene Malware-Dropper wird von Ihren Pattern-basierten Virenscannern nicht entdeckt, da er in dieser Kampagne aktuell das erste Mal verwendet wird.

Mindeststandard #1: Um möglichst viele Infiltrationsversuche Ihres Netzwerks zu erkennen, brauchen Sie einen cloudbasierten Spam-Schutz, der die Infektionswelle ohne Patterns anhand der vielen gleichartigen Mails an verschiedene Empfänger in unterschiedlichen Firmen erkennt. Idealerweise werden Links in E-Mails von diesem Schutzsystem ausgetauscht und auf ein Sicherheitssystem umgeleitet. Prüfen Sie die E-Mail-Hygieneoptionen Ihres Providers und lizensieren Sie diese möglichst vollumfänglich.

Mindeststandard #2: Gefährliche Attachments werden an Ihren Mailfiltern geblockt. Dazu gehören auch die alten Office-Formate, die mittlerweile seit 11 Jahren nicht mehr der Standard sind.

ii. Client Hardening

Die Erstinfektion findet meist an einem Arbeitsplatzrechner statt. Auch im Verlauf des folgenden, meist manuell mittels Remote Access Trojaner gesteuerten, Angriffs dienen schlecht gesicherte Client-PCs als Sprungbrett zu erhöhten Rechten.

Mindeststandard #3: Es existiert keine Möglichkeit, dass Makros in Office Dokumenten, die aus dem Internet heruntergeladen, per E-Mail oder sonst von extern empfangen wurden, auf einem Ihrer Clients ausgeführt werden. Diesen Standard können Sie durch Filtern am Perimeter oder entsprechende Konfiguration am Client umsetzen.

Mindeststandard #4: Um den Angreifern das Springen innerhalb Ihrer IT-Landschaft („lateral movement“) zu erschweren, haben Ihre Clients KEINEN einheitlichen lokalen Administrationsaccount

mit dem gleichen Passwort. Wenn Support-Userkonten notwendig sind, haben diese auf jedem Rechner ein getrenntes Passwort (das z.B. auf einem Passwortzettel im Safe hinterlegt ist).

Mindeststandard #5: Kein Benutzer arbeitet mit einem Benutzerkonto das lokale Administratorrechte hat. Aus Sicherheitssicht ist es durchaus akzeptabel, dass die Benutzer ein zusätzliches personalisiertes, lokales Administrationskonto für Ihren Rechner haben. Dieses darf aber nicht zur täglichen Arbeit benutzt werden.

Mindeststandard #6: Sie haben die Microsoft Security Baselines für Windows 10 (inklusive Office) durchgearbeitet und so viele der Empfehlungen wie möglich umgesetzt. Ebenso haben Sie Härtungsanleitungen für MacOS-Geräte, iOS (iPhone, iPad) und Android durchgearbeitet, soweit diese Geräte innerhalb des WLAN verwendet werden.

iii. Zugänge von außen kontrollieren

Mindeststandard #7: Für alle von außen erreichbaren Administrationsoberflächen ist eine MultiFaktor-Authentisierung eingerichtet. Für alle Remote-Zugänge, die danach relativ frei auf wichtige interne Ressourcen zugreifen können (RDP, Citrix, VPN) ist entweder eine Multi-Faktor Authentisierung standardmäßig oder auf Basis einer „risk based"-Loginpolicy aktiviert. Gleiches gilt wenn möglich für externe Cloud-Services wie E-Mail Konten, Dropbox, OneDrive, etc. auch hier muss MFA aktiviert werden, Dienste bei denen kein MFA möglich ist sollten wenn möglich abgeschaltet werden (IMAP, POP, etc.).

iv. Offline-Backup

Am Ende kann man nicht jeden Angreifer aufhalten. Ein gut funktionierendes Backup ist wie das Sicherungsnetz eines Hochseilartisten – man hofft, dass man es nie braucht. Falls es aber doch dazu kommt, ist es oft die einzige Überlebensgarantie.

Mindeststandard #8: Es existiert ein komplettes Backup das zu keinem Zeitpunkt älter als 7 Tage ist. Das Backup enthält neben alle wichtigen Daten.

Mindeststandard #9: Dieses Backup kann von einem Angreifer von keinem Rechner aus gelöscht werden. Die Verwaltung des Backups erfolgt mit einem getrennten Backup-Admin dessen mindestens 20 Zeichen langes Passwort in einem Safe liegt.

Mindeststandard #10: Die Ausführung der Backup-Jobs wird überwacht. Fehlgeschlagene Backups alarmieren die Verantwortlichen.

vi. Erkennung von Angriffen im internen Netz

Mindeststandard #11: Die Protokollierungsoptionen sicherheitsrelevanter Events sind auf allen Servern durchgearbeitet worden und auf – im Falle eines Sicherheitsvorfalls - hilfreiche Einstellungen konfiguriert.

Mindeststandard #12: Alle Server und idealerweise auch alle Clients müssen eine Endpoint Detection & Response Software (EDR, XDR) installiert haben. Ob Sie dabei Defender for Endpoint, Sentinel One, Crowdstrike, Black Carbon oder das AddOn Produkt Ihres Anti-Malware Herstellers verwenden ist dabei relative egal. Wichtig ist, dass Ihre IT / Ihre Dienstleister sich damit auskennen.

Mindeststandard #13: die obigen Protokollierungen müssen so konfiguriert sein, dass kritische Alarme sofort an die IT-Verantwortlichen bzw. Hauptnutzer zugestellt werden. Eine sporadische (z.B. monatliche oder quartalsweise) Durchsicht der Protokolle muss stattfinden.

vii. Patchmanagement

Die Angreifer nutzen selten komplexe Zero-Day-Lücken. Zumeist werden bestehende, teils zwei oder drei Jahre alte Lücken benutzt, die an einigen Systemen noch nicht gepatcht sind.

Mindeststandard #14: Alle Windows Systeme (Server & Clients), NAS-Server, Macs, Mobilgeräte und alle sicherheitskritischen Netzwerkkomponenten wie Firewalls, WLAN-Access Points, Router und Switches sind spätesten 10 Tage nach Erscheinen des Updates auf dem aktuellen Patchlevel. Komponenten die nicht mehr aktualisiert werden können, müssen ausgetauscht werden.

Mindeststandard #15: Alle Programme, die Daten aus dem Internet direkt verarbeiten bzw. standardmäßig Dateien öffnen, die aus dem Internet heruntergeladen werden, unterliegen einem automatischen Updateprozess und sind spätestens 10 Tage nach Erscheinen des Updates auf dem aktuellen Patchlevel (z.B. mit winget (MS-Standard) oder ninite). Insbesondere der Internet-Browser wird automatisch und häufig aktualisiert. Veraltete Software, die keine Patches mehr bekommt oder nur langsam gepatcht werden kann, darf keine Daten aus dem Internet verarbeiten.

viii. Segmentierung

Die Angreifer müssen nur ein verwundbares System im Netzwerk finden. Die Verteidiger hingegen müssen alle Systeme absichern. Das ist oft nicht für alle Systeme möglich.

Mindeststandard #16: Es existiert ein Gäste-WLAN. Alle Geräte die Sie nicht selbst verwalten dürfen nur in dieses, vom restlichen Netzwerk abgetrennte Gast-Netzwerk.

Mindeststandard #17: Technische Systeme die einen LAN oder WLAN Zugang brauchen, die aber schlecht gewartet werden oder nur selten aktualisiert werden (z.B. Kameras, Fernseher oder sonstige IoT-Geräte) werden entweder nur ins Gast-Netzwerk oder in ein weitgehend abgeschottetes IoT-Segment aufgenommen.

Mindeststandard #18: Wenn im Hauptnetzwerk besonders schützenswerte Firmendaten aufbewahrt werden (Zugangsdaten zu Vermögenswerten, größere Bitcoinbestände, streng vertrauliche Firmeninformationen), dann müssen berufliche und private Nutzung voneinander getrennt werden und das Netzwerk entsprechend auch in zwei Teile geteilt werden.

Auf diese Weise entstehen an der Firewall bis zu vier getrennte Segmente (Gast, IoT, Privat, Firma) zwischen denen die Kommunikation nur nach ganz klar definierten Regeln möglich ist.

ix. Vorbereitung auf den Ernstfall

Im Fall der Fälle wollen Sie einen Partner an Ihrer Seite haben, der bereits öfter solche Situationen gemeistert hat.

Mindeststandard #19: Lassen Sie die Sicherheitskonfigurationen und die Einhaltung dieser Regeln einmal im Jahr, spätestens aber zweijährlich überprüfen.

Mindeststandard #20: Sie haben Kontakt zu einem erfahrenen Response Consultant hergestellt und eine eventuelle Beauftragung geklärt. Das BSI führt eine „Liste der qualifizierten APT-Response Dienstleister“ und ihre Cyber-Versicherung hat eventuell auch Empfehlungen für Sie. Optional haben Sie bereits ein Krisenhandbuch für solche Fälle und eine Notfall-Whitelist für die Internetzugänge. Wenn Sie diese Prozesse dann bereits im Unternehmen einmal geübt haben, dann sind Sie ganz vorne.

Nicht verhandelbar

Um eine IT-Umgebung fit zu machen für die Abwehr von Ransomware, sind die obigen Empfehlungen ein nicht-verhandelbarer „Mindeststandard“. Es sind die Vorgaben, die ohne Wenn und Aber in jeder IT-Landschaft komplett umgesetzt sein müssen, um einen wirksamen Schutz zu etablieren.