33 technische Mindeststandards für 2023

Eine Zertifizierung nach ISO27001 schützt Ihr Unternehmen nicht vor Ransomware-Angriffen. Für viele Angehörige der IT-Sicherheitsbranche ist diese Aussage nichts Neues. Im Management der Unternehmen ist die Sichtweise oft anders: eine Anstrengung, die so viel des Sicherheitsbudgets eines Unternehmens verschlungen hat, muss auch gegen die derzeit häufigste Bedrohung nützlich sein. Die Ursache der Ineffektivität liegt jedoch in den wenig konkreten bzw. nicht-existenten technischen Vorgaben der ISO27001 und ISO 27003, den Durchfallquoten bei den Zertifizierungen, die nahe Null liegen und den oft auf einer Meta-Ebene formulierten Maßnahmenempfehlungen.

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 aber der absolute Mindeststandard, den eine IT-Sicherheitsabteilung leisten muss. Unabhängig von erworbenen Sicherheitszertifikaten muss die IT folgende Mindestanforderungen erfüllen, um die Blamage eines erfolgreichen Ransomware-Angriffs zu vermeiden. Diese Liste wird regelmäßig ergänzt und geändert und dann in der Zeitschrift <kes> veröffentlicht.

E-Mail & 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 E-Mail sieht so echt aus, dass Ihre Benutzer den Anhang 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 einem einfachen Antivirus häufig nicht entdeckt, da er in dieser Kampagne das erste Mal verwendet wird und dem Scanner unbekannt ist.

Mindeststandard #1: E-Mail-Systeme kommunizieren mit dem Internet, mit den Handys der Mitarbeiter und haben damit viele offene Schnittstellen. In der Vergangenheit haben sich diese Systeme (insbesondere ein lokaler Exchange-Server) für das lokale Netzwerk immer wieder als Einfallstor erwiesen. Der sichere Betrieb eines on-premise E-Mail Servers bindet viele Ressourcen, die in der Verteidigung an anderer Stelle besser eingesetzt werden. Wenn Sie keinen ausgezeichneten Grund dagegen haben, sollte Ihr E-Mail-System als externer Dienst (Software as a Service) eingekauft werden. Achten Sie dabei darauf, dass Ihr Anbieter über gute Sicherheitsmaßnahmen verfügt und eine MFA-Authentifizierung der Benutzer ermöglicht. Microsoft 365 Exchange Online bietet sich für viele durch einen leichten Migrationspfad an.

Mindeststandard #2: Um möglichst viele Infiltrationsversuche Ihres Netzwerks zu erkennen, brauchen Sie einen cloudbasiertes Email-Sicherheitssysteme, das die Infektionswelle anhand der vielen gleichartigen Mails an verschiedene Empfänger in unterschiedlichen Firmen erkennt. Zusätzlich müssen externe Links in E-Mails von diesem Schutzsystem ausgetauscht und auf ein Sicherheitssystem umgeleitet werden. Prüfen Sie die E-Mail-Hygieneoptionen Ihres Providers und lizenzieren Sie diese möglichst vollumfänglich.

Mindeststandard #3: Gefährliche Anhänge werden an Ihren Mailfiltern geblockt. Dazu gehören auch die alten Office-Formate, die mittlerweile seit 11 Jahren nicht mehr der Standard sind. Im Idealfall erlauben Sie nur bestimmte Dateianhänge im Stile einer Whitelist.

Mindeststandard #4: Es ist sichergestellt, dass automatische externe E-Mail-Weiterleitungen regelmäßig kontrolliert werden, damit ein Angreifer sich so keine Hintertür schaffen kann (z. B. an einem nicht gesperrten PC oder Mobiltelefon).

Client Hardening

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

Mindeststandard #5: 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. Im Idealfall blockieren Sie Makros in den Office-Programmen generell. Dies ist auch der aktuelle Standard in den Microsoft Programmen. Wenn einzelne Benutzer Makros benötigen, kann die Funktion für diese freigeschaltet werden. Aber auch solche Anwender dürfen nur Makros ausführen, die vom Unternehmen selbst signiert wurden.

Mindeststandard #6: 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 in der Domäne notwendig sind, die regelmäßig auf den Clients arbeiten, sind diese in Ihren Rechten weitgehend eingeschränkt und deren Aktionen im Netzwerk werden engmaschig überwacht. Idealerweise haben Sie Microsoft LAPS eingeführt und keine zentralen Support- oder Serviceaccounts. Dazu müssen Sie auch alle Automatisierungstasks auf Clients (z. B. Software Deployment / Inventarisierung) auf Produkte umstellen, die Agentenbasiert arbeiten und kein zentrales AD-Konto benötigen, das auf allen Clients lokaler Admin ist. Auch der User Helpdesk muss dazu auf Verfahren umgestellt werden, die keinen impliziten lokalen Admin-Zugriff erfordert (z. B. TeamViewer, Anydesk oder Microsoft Remote Help). Bei Bedarf können Helpdesk-MA das LAPS-Kennwort des jeweiligen Clients verwenden.

Mindeststandard #7: Kein Benutzer arbeitet mit einem Benutzerkonto, das lokale Administratorrechte hat. Aus Sicherheitssicht ist es akzeptabel, dass die Benutzer ein zusätzliches personalisiertes, lokales Administrationskonto für Ihren Rechner haben. Dieses darf aber nicht zur täglichen Arbeit benutzt werden und sollte daher keinen Zugang zu Unternehmensressourcen (Domäne, Fileserver, E-Mail) und (wenn möglich) auch keinen Internetzugang haben.

Mindeststandard #8: Sie haben die Microsoft Security Baselines für Windows 10 / 11, Office und Edge durchgearbeitet und so viele der Empfehlungen wie möglich umgesetzt. Für alle Empfehlungen, die Sie nicht umgesetzt haben, existiert eine Begründung. Optional haben Sie zusätzlich ein Application Whitelisting im Einsatz (z. B. Microsoft Applocker, WDAC).

Mindeststandard #9: Das BIOS aller PCs ist mit einem individuellen Passwort (z. B. abgeleitet aus der Serien- oder Inventarisierungsnummer) geschützt. Alle PCs, die die entsprechenden Hardware-Voraussetzungen mitbringen, werden unter Windows 11, als Notlösung übergangsweise mit Windows 10 mit aktivierter Virtualisierungs-basierter Sicherheit und Secure Boot betrieben. Dazu ist das BIOS entsprechend konfiguriert.

Zugänge von außen kontrollieren

Mindeststandard #10: Für alle von außen erreichbaren Administrationsoberflächen ist eine Multifaktor-Authentisierung eingerichtet. Für alle Remote-Zugänge, die danach relativ frei auf wichtige Firmenressourcen zugreifen können (RDP, Citrix, VPN) ist entweder eine Multi-Faktor Authentisierung standardmäßig oder auf Basis einer „risk based“-Loginpolicy aktiviert. Eine Bindung

des Zugriffes an Unternehmensgeräte, bekannte Geräte oder „compliant“ gesicherte Geräte ist empfohlen.

Mindeststandard #11: Die externe Auflösung von DNS-Adressen erfolgt über einen Responder, der kritische DNS-Tunnel blockiert (z. B. Quad9). Alternativ ist eine anderweitige Absicherung der DNS-Infrastruktur (z. B. keine Internet DNS Auflösung am Client/Server, nur am Proxy) implementiert. Über Firewall-Regeln wird sichergestellt, dass eine Auflösung daran vorbei nicht möglich ist.

Offline-Backup

Am Ende kann man nicht jeden Angreifer aufhalten. Es ist etablierte Vorgehensweise der Cyberkriminellen, Backupsysteme zu verschlüsseln oder zu löschen. Ein gut geschütztes und zuverlässiges Backup ist wie das Sicherungsnetz eines Hochseilartisten – man hofft, dass man es nie benötigt. Falls es aber doch dazu kommt, ist es oft die einzige Überlebensgarantie für das verschlüsselte Unternehmen.

Mindeststandard #12: Es existiert ein komplettes Backup Ihrer IT, das zu keinem Zeitpunkt älter als 7 Tage ist. Das Backup enthält neben allen Servern und Datenbanken u. a. eine Kopie des Active Directory (genauer gesagt des System States eines DC). Für die erstellten Backups existiert ein regelmäßig getesteter Wiederherstellungsplan.

Mindeststandard #13: Das Backup kann von einem Angreifer mit Domain-Admin-Rechten und Zugriff auf die Passwörter sämtlicher Domänen-Accounts nicht gelöscht werden. Typische Bausteine bzw. Ideen zur Umsetzung dieser Anforderung sind:

- Das Backupsystem steht in einem per Firewall abgetrennten Netzwerksegment und die zugehörigen Systeme sind nicht Teil der Domäne. Administrativer Zugang ist ausschließlich über Jump-Host mit lokalen Benutzern möglich (keine Domänenkonten), idealerweise mit MFA gesichert.
- Auf dem Backupsystem (bzw. dessen Storage) werden Snapshots erzeugt, die ein Administrator nur mit physischem Zugangausschalten oder löschen kann. Diese reichen weit zurück.
- Die Backups werden regelmäßig auf ein Tape geschrieben, das von einem Administrator nicht überschrieben (und damit gelöscht) werden kann.
- Die Backups werden regelmäßig in die Cloud (z.B. Azure Active Storage, AWS-Glacier) oder ein externes Rechenzentrum transferiert. Einmal transferiert, kann ein Administrator diese Backups nicht vor Ablauf der eingestellten Vorhaltezeit (mindestens 90 Tage) endgültig löschen.
- Die Backups werden regelmäßig auf einen mobilen, lokalen Datenspeicher transferiert, der dann vom Netzwerk getrennt wird.

Mindeststandard #14: Die Ausführung (und Konfiguration) der Backup-Jobs wird überwacht. Sind erfolgreiche Backups plötzlich sehr klein, oder werden gar keine Daten mehr gesichert n, fällt dies am nächsten Werktag auf und wird als Security Incident behandelt.

Domäne schützen

Mindeststandard #15: Das Ziel der Angreifer ist es, Ihre Domäne zu übernehmen. Dazu holen sich die Angreifer mit einem unprivilegierten Domänenbenutzer Account Informationen über die Schwachstellen in Ihrer Konfiguration mittels Tools wie Bloodhound. Es scheint selbstverständlich, dass Sie die gleichen Informationen haben sollten. Führen Sie einen Scan Ihrer Domäne mit dem „Healthcheck“- Tool von https://pingcastle.com (kostenfrei) durch und analysieren und beheben Sie die roten Ergebnisse.

Mindeststandard #16: Ihre Administratoren haben drei getrennte Accounts: User-, Admin- und Domain-Admin-Account mit jeweils unterschiedlichen Passwörtern. Der Einsatz von trivialen

Passwörtern wird technisch verhindert. Die Passwörter für die Admin-Accounts unterliegen besonders strengen Vorgaben. Es gibt keine Service-Accounts mit Domain-Admin Rechten. Selbstverständlich werden im Normalbetrieb nur personalisierte Administrationskonten verwendet.

Mindeststandard #17: Alle Domain Controller im Netzwerk sind ausschließlich Domain Controller und haben keine weiteren Zusatzaufgaben (außer DHCP & DNS). Alle Domain Controller sind spätestens 2 Tage nach Erscheinen eines neuen Microsoft Sicherheitsupdates auf dem aktuellen Patch-Level.

Mindeststandard #18: Die Protokollierung sicherheitsrelevanter Events wird auf allen Servern und Domain Controllern sinnvoll konfiguriert. Auf allen Domain Controllern werden auch neu gestartete Prozesse geloggt, z. B. mit dem Microsoft Tool Sysmon. Die Domäne wird umfassend auf Angriffe gegen Identitäten überwacht, z. B. mittels Defender for Identity.

Mindeststandard #19: Es existiert ein umgesetztes Konzept zur sicheren Administration, dass es einem Angreifer möglichst schwer macht, Domain-Admin Rechte zu bekommen. Idealerweise werden die Microsoft Empfehlungen zum AD Administrative Tier Model umgesetzt. Dazu teilen Sie Ihre IT in 3 Teile: Tier 0 sind alle Geräte, die die gesamte IT lahmlegen könnten (Domaincontroller, Backupsysteme, Verwaltungsrechner der virtuellen Maschinen, Firewallmanagement, etc.), Tier 1 sind alle Server, Tier 2 alle Clients. Alternativ existiert ein „red forest“-Konzept zur sicheren Administration der Hauptdomäne von einer hochabgesicherten, getrennten Admin-Domäne aus. Im Notfall reicht aber auch der Einsatz von non-domain-joined Bastion-Hosts zur Domänenadministration aus.

Mindeststandard#20: Hoch-privilegierte (Service-)Konten sind auf die minimal erforderlichen Rechte reduziert und dürfen nie Domainadministrator sein.. Dienste-Konten sind auf die minimal benötigten Rechte eingeschränkt und werden aktiv verwaltet. Hoch-privilegierte (Service-)Konten werden nur auf gesicherten Systemen („Privileged Access Workstations“) und nie auf normalen Clients verwendet. Optional existiert zusätzlich ein „Privilege Access Management System“ wie CyberARK oder Microsoft PIM.

Erkennung von Angriffen im internen Netz

Während ein Angreifer früher noch 3–4 Tage benötigte, um sich Domain-Admin-Rechte zu verschaffen, gehen die Angreifer derzeit sehr konzentriert und schnell vor. Den aktuellen Geschwindigkeitsrekord hält zurzeit die Gruppe hinter dem Verschlüsselungstrojaner RYUK, die zwei Stunden nach dem Klick eines Users auf eine Phishing-Mail Domain Admin Rechte und binnen fünf Stunden nach dem Klick das Netzwerk verschlüsselt hatten. In nahezu jedem unserer Fälle waren Spuren des Angriffs in den Protokolldateien vorhanden – sie wurden nur nicht als solche erkannt.

Mindeststandard #21: Die Verbindung der Angreifer in Ihr Netzwerk sind sogenannte Command & Control Verbindungen (C2). Ihre Firewall muss die Reputation von Zielen prüfen, bekannten C2 Adressen erkennen, ausfiltern und loggen. Des Weiteren müssen neue Verbindungen, die häufig und regelmäßig (z. B. im Minutentakt) kleine Datenmengen übertragen, an den Firewalls als verdächtig geloggt werden. Zusätzlich muss die Übertragung großer Datenmengen als verdächtig alarmiertwerden.

Mindeststandard #22: Alle sicherheitsrelevanten Logdateien werden an 365 Tagen im Jahr morgens und abends auf unerlaubte Logins, Anomalien und Angriffe geprüft. Dazu zählen insbesondere die Firewall-Logs, die Logs der Emailsicherheit und Ihres Malwareschutzes, die Logs der Domain Controller und Ihres Backupsystems. Sie können sich diese Arbeit durch die Implementierung eines Logauswertesystems mit Alarmingkomponenten erleichtern (Graylog, Elastic-Logstash-Kibana, Splunk, QRadar, etc.) oder die Arbeit komplett an ein externes Security Operation Center (SOC) outsourcen.

Mindeststandard #23: 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 Add-on Produkt Ihres Anti-Malware-Herstellers verwenden ist dabei relativ egal. Wichtig ist, dass Ihre IT sich damit auskennt und Ihr SOC das Tool stringent überwacht. Der Einsatz einer solchen Software muss ggf. mit dem Betriebsrat abgestimmt werden. Aktuell raten wir davon ab, EDR-Clients mit „Live Response"-Fähigkeiten auf Tier-0-Systemen zu installieren, da sonst ein Angriff auf das sehr mächtige EDR-System selbst kaum zu beherrschen ist. D. h. für Tier-0-Systeme haben Sie nur die Überwachung aus den Mindeststandards #10, #14, #16 , #17 und #22

Patch Management

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. Wenn ein Sicherheitsproblem einen CVSS-Score >= 7.0 hat, dann ist die Kritikalität „high".

Mindeststandard #24: Alle Windows Systems (Server & Clients) sind spätesten 10 Tage nach Erscheinen eines Updates mit Kritikalität „high" auf dem aktuellen Patch-Level. Alle anderen Updates sind spätestens nach 30 Tagen eingespielt.

Mindeststandard #25: Alle Programme, die Daten aus dem Internet direkt verarbeiten oder standardmäßig Dateien öffnen, die aus dem Internet heruntergeladen werden, unterliegen einem automatischen Updateprozess und sind spätestens 10 Tage nach Erscheinen eines Sicherheitsupdates mit Kritikalität „high" auf dem aktuellen Patch-Level. Alle anderen Updates sind spätestens nach 30 Tagen eingespielt. 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. Software, die nicht mehr gewartet und gepatcht wird, darf maximal noch 3 Monate weiterlaufen. Der Austausch solcher Software ist ein Unternehmensprojekt höchster Priorität.

Netzwerksegmentierung

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 #26: Systeme, die die obigen Regeln nicht einhalten können und/oder unsichere Protokolle (wie SMBv1) verwenden müssen, werden vom Netzwerk isoliert und in ein eigenes, von einer Firewall gegenüber dem restlichen Netz abgetrenntes Netzwerksegment verbracht. Die Systeme müssen auch aus der Windows-Domäne entfernt werden, ansonsten ist die Segmentierung nutzlos.

Mindeststandard #27: Systeme, die einen höheren Sicherheitsstandard benötigen (z. B. Produktionssteuerungen, Industrie 4.0) oder nicht so gut kontrolliert werden können (z. B. Entwickler-Testnetzwerke, Lokationen ohne IT-Durchgriff, IoT- und Haussteuerungsnetzwerke) müssen netzwerktechnisch segmentiert und in getrennten Domänen betrieben werden. Vertrauensstellungen zwischen den Domänen dürfen nur einseitig von der sicherheitstechnisch weniger kritischen zur kritischeren Domäne existieren, nicht umgekehrt. Die Netzwerksegmentierung erfolgt über eine Firewall. Wo möglich (z. B. Produktion) erhalten die Segmente nur per Whitelist eingeschränkten Zugang ins Internet. Die Verbindungen zwischen den Segmenten sind auf das notwendige Minimum von Ziel-IP/Port Kombinationen beschränkt.

Mindeststandard #28: Die Trennung Ihrer IT in 3 Teile nach Mindeststandard #19 sollte sich auch auf der Netzwerkebene in der Segmentierung wiederfinden. Freien Internetzugang zu beliebigen Zielen erhält nur Tier 2, Tier 0 und 1 dürfen nur zu dedizierten Zielen Verbindungen aufnehmen („Internet

Whitelisting“). Eingehende Verbindungen (vom Internet und untereinander) sind je Tier streng reglementiert und auf das Notwendige beschränkt.

Virtualisierungsinfrastruktur

Die Angreifer nutzen vermehrt einen direkten Zugriff auf die Virtualisierungsinfrastruktur (insbesondere VMware vSphere ESXi-Hosts), um alle virtuellen Maschinen auf einmal zu verschlüsseln.

Mindeststandard #29: Domänenkonten werden nicht für Administrator Level Zugriffe auf Ebene der Virtualisierungsverwaltung (z. B. vSphere, vCenter) verwendet. HyperV wird entweder mit Anschluss an eine dedizierte, gesicherte Management-Domäne ohne Anschluss an die normale Office-Domäne betrieben, oder ohne Domänenanschluss. In allen Fällen werden sichere Passwörter für administrative Konten benutzt, die nirgendwo anders verwendet werden. Datenverkehr im virtuellen Speichernetzwerk ist ebenfalls in separaten physischen und logischen Netzwerken isoliert. Die Administrationsschnittstellen (z. B. vCenter Server und ESXi) sind nur für definierte Computer und Benutzer erreichbar (z. B. mittels Netzwerksegmentierung). Es werden nur dediziert gesicherte Workstations für die Administration verwendet.

Mindeststandard #30: Die Ausführung von benutzerdefiniertem Code ist auf Ebene des Hypervisors (z. B. ESXi – VMkernel.Boot.execInstalledOnly) eingeschränkt oder blockiert. Der administrative Zugriff auf das Betriebssystem der Virtualisierungsverwaltung (z. B. vCenter Server) ist auf das Nötigste beschränkt.

Cloud-Umgebungen

Derzeit ist von den Cloud-Umgebungen insbesondere Microsoft 365 im Blickfeld von Cybercrime Banden. Gehäuft werden dabei einzelne E-Mail-Konten kompromittiert und darüber weiterführende Angriffe (primär Phishing, Informationsdiebstahl, Payment Diversion) ausgeführt. Dies verursacht heute schon signifikante Schäden. Angriffe auf administrative Cloud-Berechtigungen sind noch eine Seltenheit, weshalb der Schutz davor derzeit noch nicht in den Mindeststandards verankert ist (aber natürlich schon durchgeführt werden sollte).

Mindeststandard #31: Für alle Konten der jeweiligen Cloud-Umgebung ist eine Multi-Faktor Authentisierung mit sinnvollen Einstellungen aktiv. Ausnahmen gelten für Emergency Access Admin Accounts („break glass accounts“) und gegebenenfalls Servicekonten, die anderweitig (z. B. sehr lange Kennwörter, API-Token, FIDO2, Einschränkung des Zugriffes auf eine einzelne IP Adresse etc.) geschützt werden müssen. Zugriffsberechtigungen für 3rd Party Enterprise Apps werden ausschließlich über Administrator Consent freigegeben, niemals durch die Anwender direkt.

Vorbereitung auf den Ernstfall

Im Fall der Fälle wollen Sie einen Partner an Ihrer Seite haben, der bereits öfter die Krisen und Nöte nach einem erfolgreichen Ransomwareangriff gemeistert hat.

Mindeststandard #32: Sie haben Kontakt zu einem erfahrenen Response-Consultant hergestellt und eine zeitnahe Unterstützung im Notfall 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 businesskritischer Webseiten und Gegenstellen für die Einschränkung der Internetzugänge vorbereitet. Wenn Sie diese Prozesse dann bereits im Unternehmen einmal geübt haben, dann sind Sie ganz vorn.

Sollte der Notfall eintreten, möchten Sie den Angriff nachvollziehen und forensisch untersuchen können.

Mindeststandard #33: Alle Log- und Protokollierungseinstellungen in der Infrastruktur sind so angepasst, dass eine Aufklärung von Sicherheitsproblemen möglich ist. Angriffe laufen selten nur über ein System. In einen erfolgreichen Angriff sind – neben dem eigentlichen Zielsystem – meist verschiedene andere Systeme involviert, mit deren Hilfe der Angriff vorbereitet wird („Stagingsystem“). Falls ein System als Stagingsystem in einem Angriff beteiligt war, muss der Pfad des Angriffs zum vorhergehenden und dem nachfolgenden System nachvollziehbar sein. Für das Zielsystem eines Angriffs muss nachvollziehbar sein, wie der Angriff abgelaufen ist, um weitere Angriffe dieser Art verhindern zu können. Der wichtigste Punkt der Protokollierung ist dabei die Aufbewahrungsdauer: je öfter und intensiver in einem Unternehmen die Logdateien kontrolliert werden, desto weniger lang müssen sie aufbewahrt werden. In den meisten Unternehmen scheint eine Aufbewahrungsfrist von 90 Tagen das Minimum darzustellen – generell sollten Logdateien nie ungeprüft gelöscht werden. Wichtigste Voraussetzung für eine sinnvolle Logauswertung ist eine möglichst genaue Zeitsynchronität (<60s Abweichung) aller beteiligten Rechner. Dazu gehört auch, dass alle Systeme der Infrastruktur (Rechner, Netzwerkequipment, etc.) die gleiche Zeitzone haben. Idealerweise sollten die Logs immer mit UTC-Zeitstempeln erstellt werden. Wenn das nicht geht, muss für jedes System genau notiert werden, in welcher Zeitzone das System die Logzeitstempel erzeugt.

1.12 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. An dieser Stelle werden jetzt die CISOs – geschult durch ISO27001 - versucht sein, Abweichungen zu notieren, die im Laufe der Zeit behoben werden. Gleichzeitig werden Manager „Risikoübernahmeformulare“ aus dem Hut zaubern, Finanzabteilungen vor Kostenexplosionen warnen und IT-Administratoren mit dem Verlust der Verwaltbarkeit und Verfügbarkeit argumentieren. Wenn Sie nach einem Ransomware-Angriff zwischen den rauchenden Ruinen Ihrer infizierten Domäne, den gelöschten Backups und den verschlüsselten Servern stehen, können Sie dann über die Unsinnigkeit von notierten Abweichungen, Risikoübernahmeformularen, IT-Sparmaßnahmen und möglichst bequemer Administration sinnieren.

Außerdem helfen die obigen Maßnahmen gegen derzeitige Ransomware, die Vorgehensweisen entwickeln sich aber ständig weiter. Genug Geld für verbesserte Angriffe ist mittlerweile im System. Andere Maschen der organisierten Kriminalität wie Business-E-Mail Compromise (Payment Diversion, Fake President, etc.) erfordern nochmals ganz andere Schutzmaßnahmen, und wenn Sie einer Gefährdung durch Industriespionage oder state-sponsored actors ausgesetzt sind, dann sind nochmals weitere Maßnahmen erforderlich. Gleichzeitig gibt es noch weitere Empfehlungen, die über den obigen absoluten Mindeststandard hinausgehen, wie regelmäßige Übungen und Audits, den Aufbau von Honeypots und deren Überwachung, jährliche Revision der IT-Sicherheitssituation, effektive Awareness Maßnahmen oder die Implementierung von Netzwerksensoren.

Autor: Florian Oelmaier
Prokurist, Leiter IT-Sicherheit & Computerkriminalität, IT-Krisenmanagement
https://twitter.com/h0tz3npl0tz

CORPORATE TRUST
Business Risk & Crisis Management GmbH
Graf-zu-Castell-Straße 1
D-81829 München

Tel.: +49 89 599 88 75 80

info@corporate-trust.de
www.corporate-trust.de
blog.corporate-trust.de