DIGITAL SICHER NRW

Kompetenzzentrum für Cybersicherheit in der Wirtschaft in NRW

SPECIAL EVENT:

WAS WIR VON RANSOMWARE VORFÄLLEN LERNEN KÖNNEN

Beauftragt vom Ministerium für Wirtschaft, Innovation, Digitalisierung und Energie des Landes Nordrhein-Westfalen

EINIGE ZAHLEN UND FAKTEN ZU RANSOMWARE

der deutschen Unternehmen sehen in Ransomware die größte Bedrohung

5

In jedem 5. deutschen Unternehmen hat Ransomware bereits einen Schaden verursacht

+358%

mehr Erpressung und Systemausfälle 2019 auf 2020

223 Mrd. EUR

Gesamtkosten/-schaden durch Schadsoftware in Deutschland (Diebstahl, Spionage und Sabotage)

394.000

neue Schadprogramme täglich

Massiver Anstieg von Lösegeldforderungen

- Ransomware verschlüsselt nicht nur, sondern kann Daten auch kopieren (Erpressung mit möglicher Veröffentlichung)
- Ransomware-Gruppen sind straf-rechtlich nur schwer verfolgbar

Quellen:
https://www.bitkom.org/Presse/Presseinformation/Angriffsziel-deutsche-Wirtschaft-mehr-als-220-Milliarden-Euro-Schaden-pro-Jahr#item-8440
https://www.heise.de/news/Ransomware-Conti-Erpressergruppe-verbittet-sich-Leaks-ihrer-Verhandlungs-Chats-6206790.html
https://blog.wiwo.de/look-at-it/2021/08/23/cybersicherheit-die-wichtigsten-zahlen-fakten-zu-ransomware-im-jahr-2021/

EMOTET IST ZURÜCK

BSI: „gefährlichste Schadsoftware der Welt“

Ursprünglich 2014: Banking-Trojaner mit dem Ziel, Online-Zugangsdaten von deutschen und österreichischen Bankkunden abzufangen

Inzwischen kann Emotet Vielzahl von Modulen mit verschiedenen Schadfunktionen nachladen und ausführen → Command & Control
Werkzeugkasten: Kann fast alles und wird laufend mit neuen Fähigkeiten ausgestattet

Wichtigster Angriffs-Vektor: Spam-E-Mails mit Malware-Anhängen

EMOTET IST ZURÜCK

Emotet nutzt „Outlook-Harvesting“
– Auslesen von E-Mail Inhalten aus den Postfächern der infizierten Systeme
→ Basis für weitere Angriffe und schnelle Verbreitung

- **Spam-Modul:** Andere Empfänger erhalten authentisch wirkende E-Mails von Personen, mit denen sie tatsächlich bereits in Kontakt standen
  → URLs und Anhänge werden dann eher geöffnet
- **Wurm-Modul:** Selbstständige Verbreitung im Netzwerk

Angreifer nisten sich im System ein und bleiben möglichst lange unentdeckt und handlungsfähig

→ **Extremfall**: Datendiebstahl, Kontrollverlust, Ausfall IT-Infrastruktur

→ Ganze Unternehmensnetzwerke müssen neu aufgebaut werden

→ Vorsicht bei E-Mail Anhängen und URLs!

ÜBER DAS BETROFFENE UNTERNEHMEN

Wir haben dem betroffenem Unternehmen Anonymität versichert.

ÜBER DAS BETROFFENE UNTERNEHMEN

Standort / Region: RP/NRW

Mitarbeiter: ca. 50

Branche: Maschinenbau

ÜBER DAS BETROFFENE UNTERNEHMEN

IT Verantwortung:

Inhouse in Verbindung mit

kleinem qualifizierten

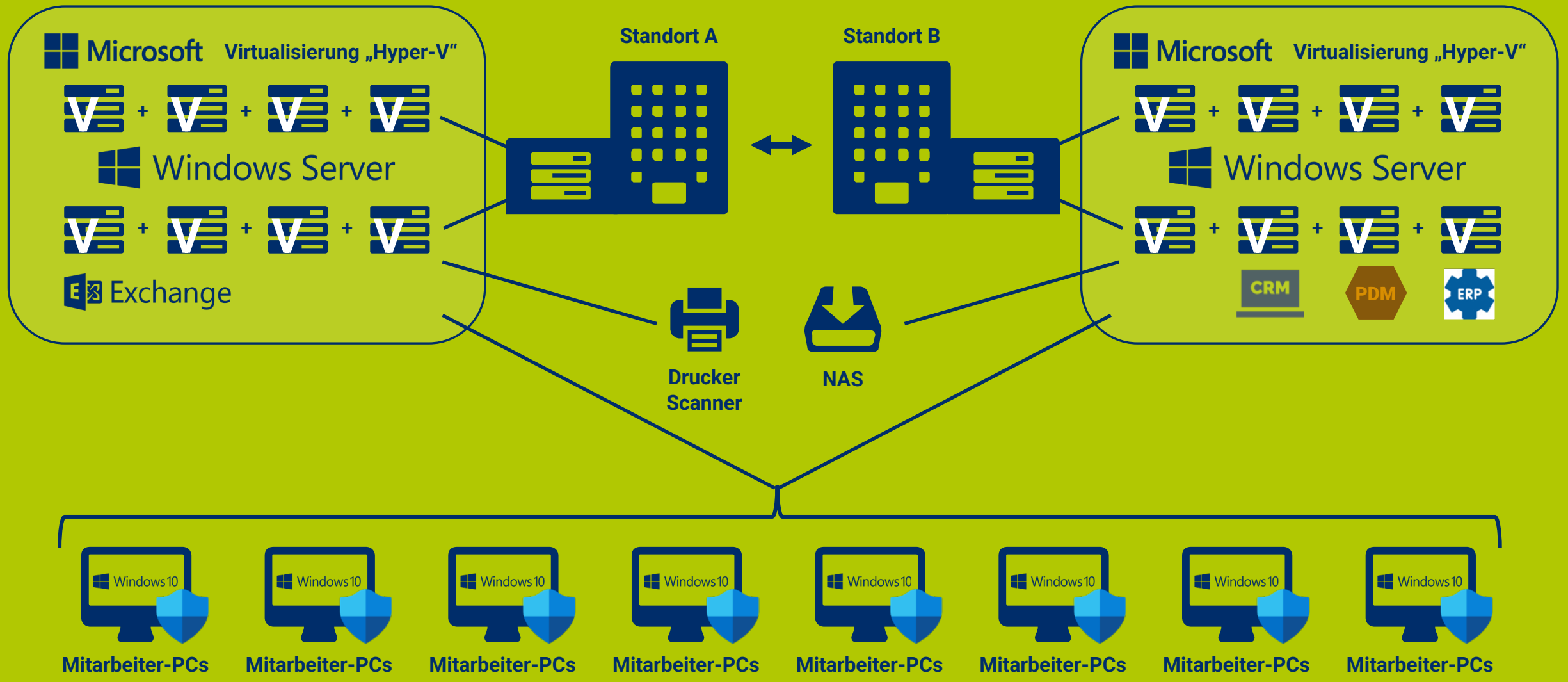
IT-Dienstleister


LETZTENDLICH:
WIR KÖNNEN WIEDER
PRODUZIEREN
UND ARBEITEN


ENTSTANDENER
SCHADEN:
BIS ZU 300.000 EURO

ABER WAS IST EIGENTLICH PASSIERT?

BESCHREIBUNG DER IT-INFRASTRUKTUR



EINGESETZTE BACKUPSTRATEGIE

Backup-Software: Veritas Backup Exec

- Täglich: Inkrementelle Datensicherungen
- 1x pro Woche (am Wochenende) Vollbackup
- 1x pro Monat: Größere Daten, die sich selten ändern
- 1x je Quartal: Archivierung von Vollbackup (4 davon werden vorgehalten in zyklischem Wechsel; offline/ nicht mit Produktiv-System verbunden)

Datenträger für Sicherungen der Backups:
Professionelles Wechselfestplattensystem

Datenträger werden im Nebengebäude aufbewahrt, um z.B. bei Brand geschützt zu sein.

Zusätzlich: Volumenschattenkopien auf Netzlaufwerken zum Schutz vor versehentlichem Löschen
→ Erlaubt schnelle Wiederherstellung ohne Zugriff auf das Backup-System

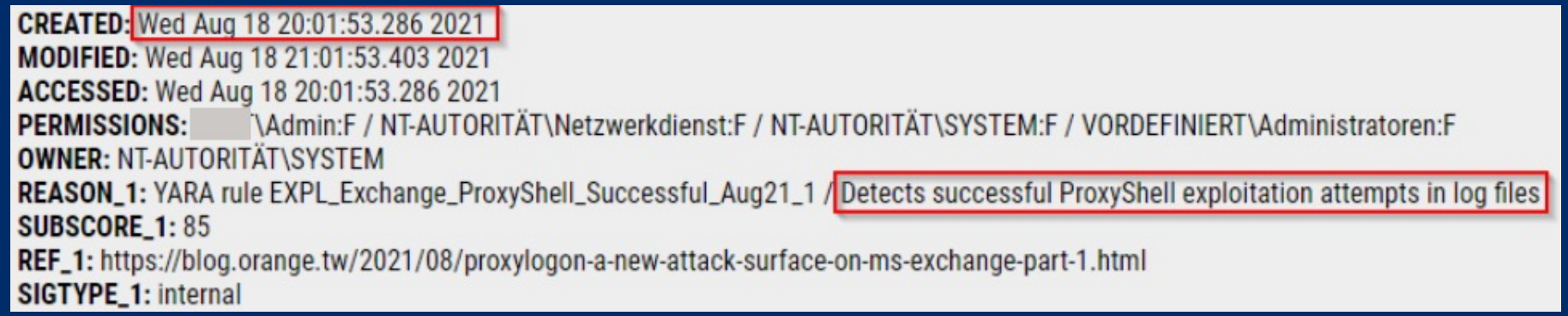
TATHERGANG

TATHERGANG

18. AUGUST - MITTWOCH

INITIALER ZUGRIFF AUF UNTERNEHMENSSTRUKTUR

- Einfallstor: Exchange Server 2016 (On-Premise)
- Ausgenutzt: „ProxyShell“-Schwachstelle
  - Updates sollten wenige Tage nach Update/Patch-Möglichkeit eingespielt werden
- Verschaffung von Zugriff auf Firmennetzwerk
  - Webshell-Skripte werden hochgeladen und ausgeführt
- Sicherheitsupdates für den Exchange Server nach dem Vorfall konnten die bereits installierte Hintertür nicht mehr schließen.



TATHERGANG

18. – 26. AUGUST

LATERAL MOVEMENT: BEWEGUNG INNERHALB DES NETZWERK

- Es werden insgesamt sechs Webshell-Skripte hochgeladen
- Weitere Details nicht bekannt

27. AUGUST - FREITAG

MANUELLER EINSTIEG DURCH ANGREIFER

- **21:27 Uhr**: abcd.exe wird in Root-Verzeichnis des Exchange-Servers geladen und entpackt.
- abcd.exe scheint ein „Multitool“ zu sein, d.h. ein Programm mit verschiedenen Funktionen (Werkzeugkasten).
    - Deaktivierung Anti-Malwarelösungen (Defender)
    - Remote Control
    - Beschaffung von Löschrechten
    - Analyse
    - Funktionen zur Fortbewegung im Netzwerk (Lateral Movement)

ANALYSE DES PROGRAMMS ABCD.EXE

TATHERGANG

27. AUGUST - FREITAG

Malware

Teamviewer-Tools

Grafikkarten-Bibliothek

Admin-Funktionalitäten

TATHERGANG

28. AUGUST - SAMSTAG

ÜBERNAHME VON WEITEREN PRIVILEGIEN

- **04:03 Uhr:** Zusätzliches Programm wird im Root-Verzeichnis des Exchange-Servers abgelegt.
- Tool ist verschleiert, dynamische Analyse nicht erfolgreich.
- Vermutlich ebenfalls selbstgeschriebenes Programm zur Erweiterung von Privilegien (Privileged Escalation) und der Bewegung im Netzwerk (Lateral Movement)

29. AUGUST - SONNTAG

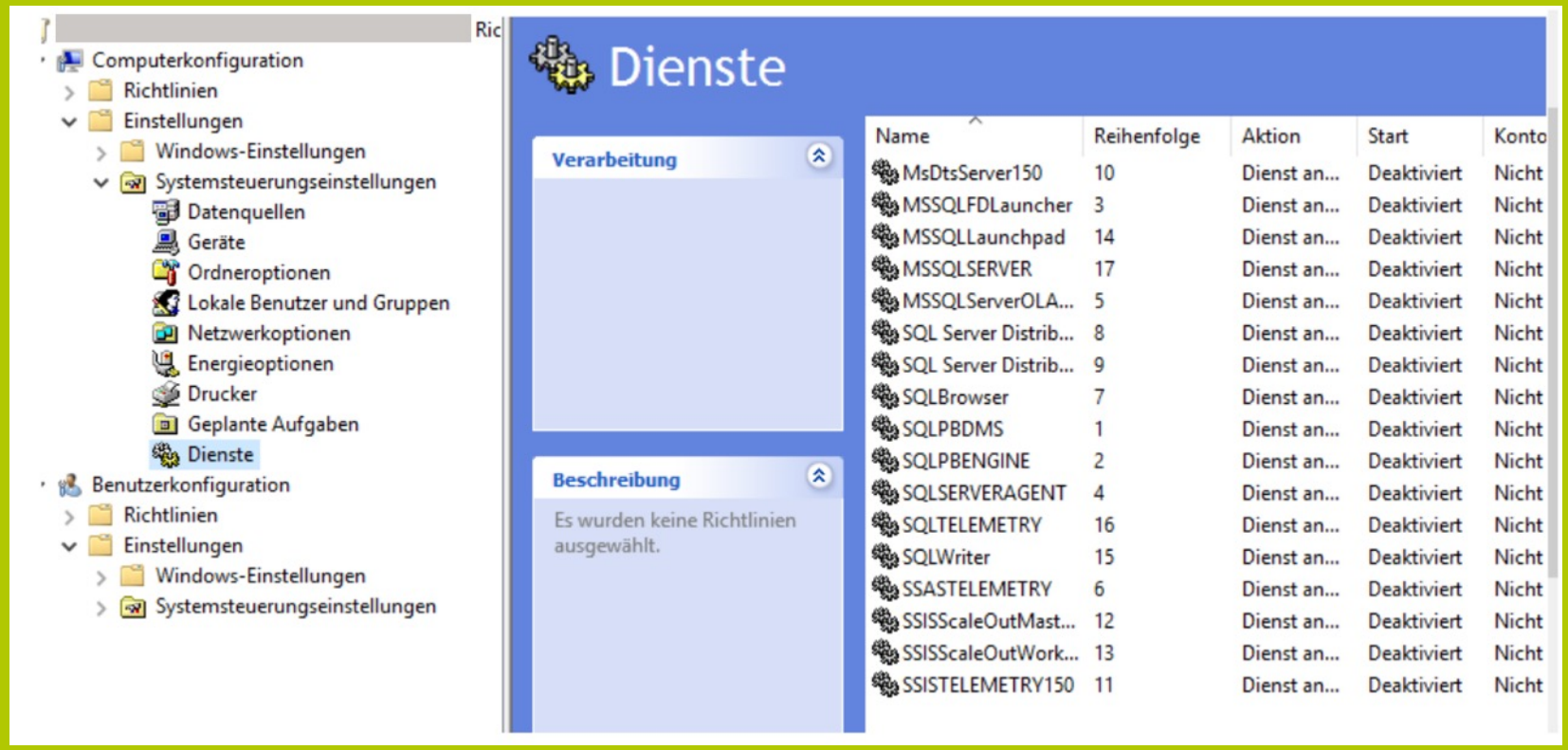
FORTSETZUNG DES ANGRIFFS IN DEN FRÜHEN MORGENSTUNDEN

- Netzwerk-Monitoring-Tool „Advanced IP Scanner“ (wurde bereits installiert), identifiziert Rechner im Netzwerk sowie den Domänencontroller.
- Ausgehend vom Exchange-Server finden wiederum Lateral Movements zu anderen Systemen statt.
- Neue Gruppenrichtlinien auf Domänencontroller erstellt und genutzt, um folgende Aktionen zu verbreiten:

TATHERGANG

1

Deaktivierung von Datenbankdiensten, um das Verschlüsseln der Datenbanken zu ermöglichen



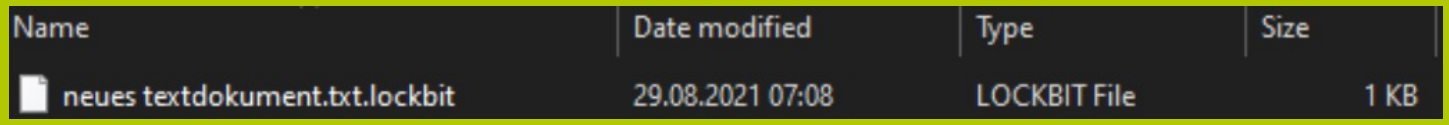
TATHERGANG

2

Sämtliche Prozesse, welche Dateien blockieren könnten, wurden beendet

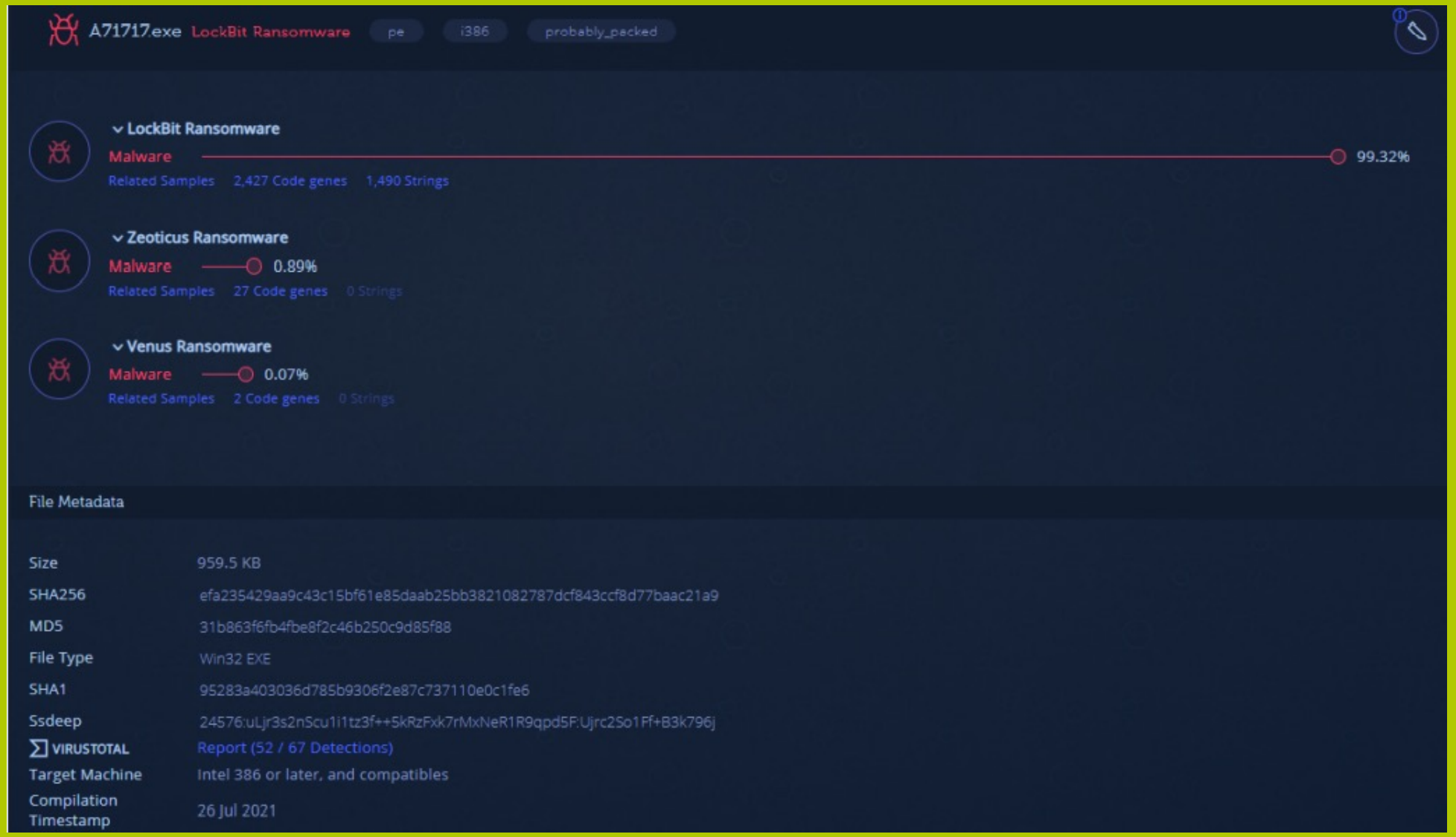
3

Zuvor eingeschleustes Verschlüsselungsprogramm (A71717.exe) wurde auf jeweilige Server/ Rechner kopiert und der Verschlüsselungsprozess gestartet.



Dynamische Analyse des Programms bestätigt: Verschlüsselungsprogramm von LockBit 2.0

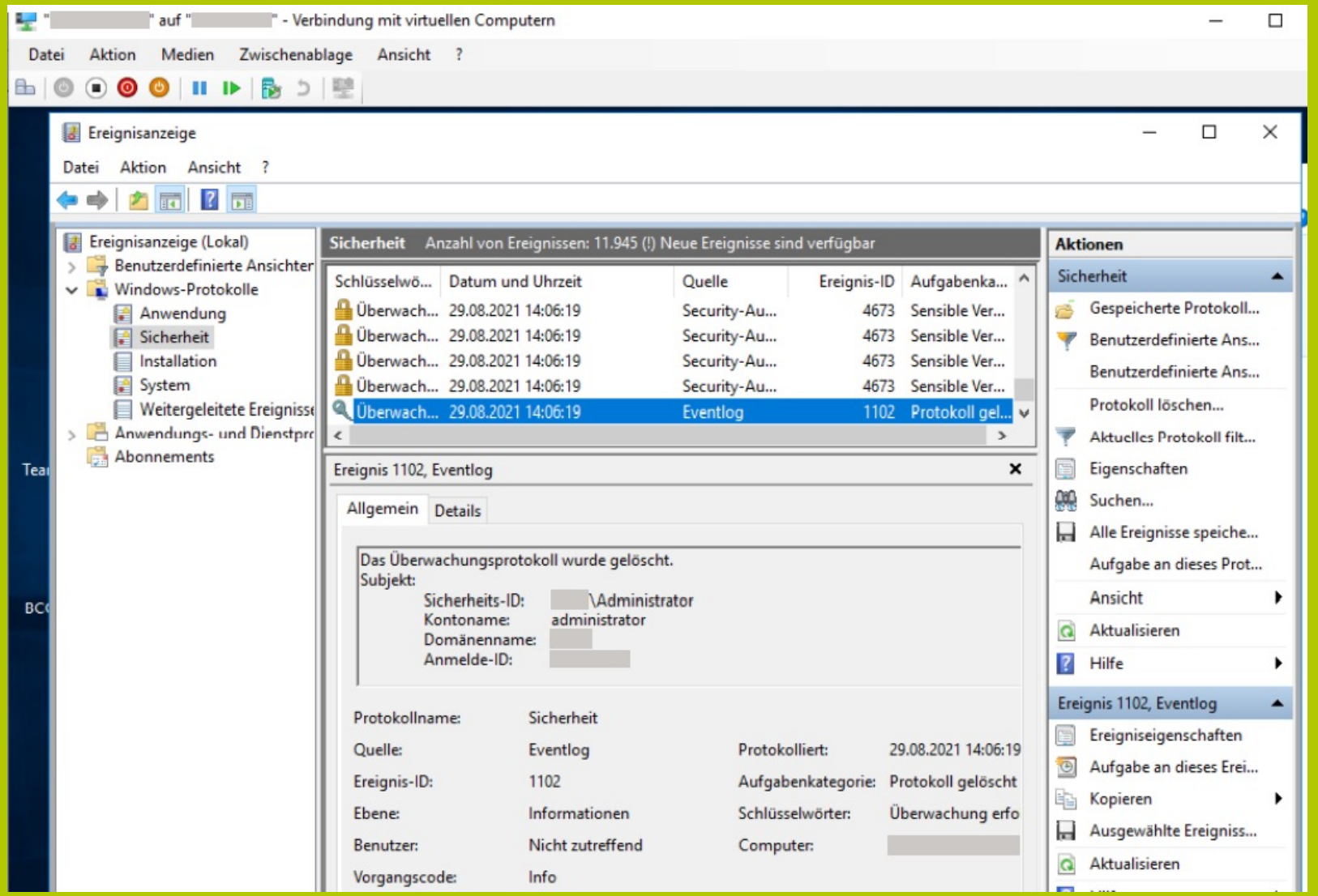
DYNAMISCHE ANALYSE DES PROGRAMMS



TATHERGANG

4

Nach Verschlüsselung der Daten löschte A71717.exe sämtliche Windows Event Logs.
(Windows Ereignisprotokoll)



TATHERGANG

5

Auf dem Desktop der verschlüsselten Rechner wurden Nachrichten als Textdatei hinterlegt.

Die letzten Aktivitäten der Angreifer wurden Sonntag, 29.8. gegen 7:00 Uhr festgestellt.

```
You can contact us and decrypt one file for free on these TOR sites
http://lockbitsup4yezcd5enk5unncx3zcy7                    .onion
http://lockbitsap2oaqhcun3syvbqt6n5nzt                    .onion
OR
https://decoding.at

Decryption ID: A717177B7AAB                    LockBit 2.0 Ransomware
```

Hinweis zur Kontaktaufnahme wurde auf allen Druckern vielfach ausgedruckt.

Es wurde kein Kontakt mit den Erpressern aufgenommen.

NACH DEM ANGRIFF

NACH DEM ANGRIFF

29. AUGUST - SONNTAG

ERSTE MASSNAHMEN

- Feststellung des Vorfalls beim Versuch, Wartung der Server vorzunehmen.
- Alle Server abgeschaltet und Geschäftsführer über Vorfall informiert.
- Verschiedene weitere Mitarbeiter informiert.
- Mitarbeiter-PCs übers Wochenende ausgeschaltet, daher nicht betroffen.
    - Kein „Wake-On-LAN“ aktiviert
- Mitarbeiter wurden informiert und durften Endgeräte nicht einschalten.

NACH DEM ANGRIFF

30. AUGUST - MONTAG

MELDUNG AN ÖRTLICHE POLIZEI UND LKA CYBER-CRIME-ABTEILUNG

- Geschäftsführer meldet Tat der örtlichen Polizei und Cybercrime-Abteilung des Landes wird über Vorgang informiert.
- Die Polizei leitet Vorgang an Kriminalpolizei weiter. Diese besucht Unternehmen noch am gleichen Tag und nimmt Logdaten mit.
- IT-Dienstleister und Mitarbeiter verschaffen Überblick über Schaden sowie über noch nicht verschlüsselte Daten.
- Externen **Datenschutzbeauftragten** wird über möglichen Datenschutzverstoß informiert.
    - Potenzielle Verstöße müssen innerhalb von 72h nach Vorfall gemeldet werden.
- Erste (virtuelle) Server auf neuer Hardware installiert.
- Scan aller Rechner im Netzwerk mit Anti-Malwarelösung „Malwarebytes“.
- Zuvor Microsoft Defender aktiv.

NACH DEM ANGRIFF

31. AUGUST - DIENSTAG

IT-FORENSISCHE ANALYSE DURCH IT SECURITY EXPERTEN

- Technischer Bericht mit kurz-, mittel- und langfristigen Empfehlungen wenige Tage später

01. SEPTEMBER - MITTWOCH

DATENSCHUTZ UND ANTI-MALWARELÖSUNG

- Erstellung von Liste von Daten von potenziell betroffenen Personenkreise (Daten von Mitarbeitern, Kunden, Partnern, usw.)
- Meldung an **Datenschutzbehörde**, da personenbezogene Daten potenziell betroffen sein könnten.
- Maßnahmen definiert, um kritisch klassifizierte Personenkreise zu informieren.
- Datenschutz-Verfahren ohne Bußgeld eingestellt, da nicht grob fahrlässig.
- Umstieg auf neue Anti-Malwarelösung “Palo Alto Cortex“

NACH DEM ANGRIFF

03. SEPTEMBER- FREITAG

UMZUG IN DIE CLOUD – WIEDERHERSTELLUNG SICHERHEITSKOPIEN

- Exchange-Server in der Cloud neu installiert und E-Mail-Accounts eingerichtet.
- Domänencontroller und Benutzer neu eingerichtet.
- Viele PCs bereits schnell wieder in der Domäne.
- ERP-System einsatzfähig / nicht verschlüsselt.
- Viele Daten mittels Sicherungskopien wieder hergestellt.

24. SEPTEMBER - FREITAG

ALLE SYSTEM WIEDER EINSATZFÄHIG

- Alle Systeme sind wieder einsatzfähig.
- Alle PCs sind mit neuer Anti-Malwarelösung versehen.

19. OKTOBER - DIENSTAG

EINSTELLUNG DES VERFAHRENS GEGEN UNBEKANNT

- Staatsanwaltschaft stellt das Verfahren gegen Unbekannt ein, da die Täter nicht ermittelt werden können.

AUSMASS DES SCHADENS – EINE BILANZ

Schaden entstanden durch

- Verlust von nicht-wiederherstellbaren Daten
  - Wiederherstellung nur von „veralteten“ Daten möglich
- Arbeitsausfall wegen nicht-vorhandener Arbeitsmittel
- Tätigkeiten im Zusammenhang mit dem Angriff
  - Unterstützung des IT-Dienstleisters, Meldung an Datenschutzbehörde, Gespräche mit Kriminalpolizei, etc.

Neuaufsetzung aller Server durch IT-Dienstleister

Kosten für Neuinstallation und Datenträger (eigene Server)

Beanspruchung weiterer Dienstleister (z.B. Neuaufsetzen des CRM-Systems)

Einige dauerhaft verlorene Daten werden sukzessive rekonstruiert.

Gesamtschaden: bis zu 300.000 EUR

DETAILS 1

Verschlüsselt

- Alle im Netzwerk aktiven Rechner/Server mit Ransomwarelösung LockBit 2.0.
- Eingelegte Datensicherungsträger.
  - Teilweise Backups mehrerer Wochen betroffen.
  - Einige Daten konnten durch lokale Sicherungen bzw. über nicht betroffene Endgeräte wiederhergestellt werden.
- Datenbanken der CRM-Software sowie des Produkt-Daten-Management-Systems.

Gelöscht

- Schattenkopien (diese greifen auf Backup zu; nur kurzfristiger „Zwischenspeicher“)

Nicht betroffene Systeme

- ERP-System / System musste nur auf neuem Server installiert werden
- E-Mails konnten bis auf wenige Ausnahmen wiederhergestellt werden
  - über lokale Sicherungen (Programmeinstellungen)
  - aus einer nicht verschlüsselten Datenbank des Exchange-Servers
- Produktionssysteme

DETAILS 2

Analyse des Tathergangs durch Mangel an Logdaten erschwert

- Systemlogs von Angreifern gelöscht
- Speicherzeitraum für Datentransferlogs auf Routern und gemanagter Firewall war deutlich zu kurz
- Anfrage bei der Deutschen Telekom: für Festnetzanschlüsse werden keine Datentransfers geloggt

Laut IT-Forensikern ist davon auszugehen, dass keine oder keine nennenswerten Datenmengen abgeflossen sind (kein Daten-Diebstahl).

- Zeitraum des finalen Angriffs zu kurz, um größere Datenmengen zu transferieren
- Beobachtung des Darknets über kommende Wochen: keine Datenveröffentlichungen

WIEDERHERSTELLUNG DES SYSTEMS – ZUSAMMENFASSUNG

Alle Server neu aufgesetzt mit neuen Festplatten

Alte Festplatten archiviert. Gründe:

- Beweissicherung
- Möglichkeit zur späteren Wiederherstellung, wenn Entschlüsselungsverfahren für LockBit 2.0 allgemein verfügbar ist (ähnliches bereits bei anderen Ransomware-Lösungen geschehen)

Sämtliche Client-Rechner mit Anti-Malwaresoftware gescannt.

Ab 1. September (3 Tage nach dem Angriff) neue Anti-Malwarelösung (Cortex, Palo Alto) installiert.

Exchange-Server (On-Premise) als Cloud-Dienst (Microsoft 365) neu aufgesetzt.

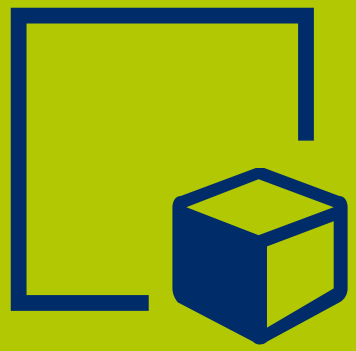
Neue Domäne unter neuem Namen.

Benutzernamen wurden nach neuem Schlüssel angelegt.

Sämtliche Passwörter geändert. Keine früher verwendeten Passwörter.

Schlüssel für VPN-Zugang erneuert.

LANGFRISTIGE MASSNAHMEN



Überdenken der gesamten IT-Strategie.

Ergänzung des IT-Dienstleisters durch IT Security Experten

oder

Wechsel zu einem anderen Anbieter, der Security-Kompetenzen besser abdeckt als der bisherige Dienstleister.

LEARNINGS AUS DEM VORFALL

1. Backups – was kann man noch besser machen?
2. Updates – mit sofortigem Update wäre Zero-Day Exploit, mit dem der Prozess begann, nicht möglich gewesen
3. Empfehlung: Längerer „Log-Zeitraum“, um Datenabflüsse nachvollziehen zu können.

WÜNSCHE AN POLITIK 1

- Aufklärungsarbeit zur Schaffung eines IT-Sicherheitsbewusstseins
  - Informationsangebote
  - Verringerung von Überforderung insb. kleinerer Unternehmen
- Hilfestellung, wie man Vorfälle in den Griff bekommt
  - Prävention und Incident Response/Vorfallsbehandlung;
- Wie kann man Unternehmen zur Umsetzung von Maßnahmen bewegen?

WÜNSCHE AN POLITIK 2

- Mehr Kompetenz und Expertise bei den Behörden, z.B. Strafverfolgung
- Kooperationen auf internationaler Ebene
  - Ausüben gemeinsamen Drucks auf Hackergruppen, z.B. um Schlüssel preiszugeben.
  - Hackergruppen dürfen sich in keinem Land sicher fühlen.

VON ANGREIFERN LERNEN

Alle Punkte wurden Verhandelnden im Rahmen einer Lösegeld-Verhandlung von einer Gruppe von Angreifenden, einer BlackHat-Gruppe, zugespielt.

VON ANGREIFERN LERNEN

Das heute vorgestellte betroffene Unternehmen hat keinen Kontakt zu den Erpressern aufgenommen.

VON ANGREIFERN LERNEN

1. Administratoren müssen in Browsern im privaten Modus arbeiten.

2. Administratoren ist es untersagt, Passwörter in Browsern zu speichern.

3. Administratoren ist es untersagt, Dateien mit Passwortlisten auf ihren Computern oder gemeinsam genutzten Ressourcen zu speichern und per E-Mail zu versenden.

4. Verdächtige E-Mails dürften nicht geöffnet werden. Wenn sie geöffnet werden sollen, muss dies in geschützter, kontrollierter Umgebung geschehen, z.B. auf Computern ohne Verbindung zum Unternehmensnetzwerk.

Alle verdächtigen E-Mails mit Links sollten an die IT-Abteilung geschickt werden, damit sie auf einer eigenständigen virtuellen Maschine überprüft werden können.

VON ANGREIFERN LERNEN

5. Administratoren arbeiten in virtuellen Maschinen. Virtuelle Maschinen müssen in Kryptocontainern untergebracht werden.

6. Firewalls müssen so konfiguriert werden, dass die Computer der Administratoren keinen direkten Zugang zu kritischen Servern haben, die virtuellen Maschinen jedoch schon (Firewall-Regeln und Netzwerkbereiche).

7. Beschränken Sie die Liste der Domänenadministratoren. Das Domänenadministrator-Passwort sollte zwischen Sicherheitsabteilung und Verwaltungsabteilung aufgeteilt werden (das Passwort ist sehr lang).

8. Teilen Sie die Verantwortung so auf, dass verschiedene Administratoren unterschiedliche Rechte haben und verwalten (kleine, regelmäßige Aufgaben wie Zurücksetzen von Passwörtern, Anlegen von Benutzern wird weniger restriktiv gehandhabt als tiefergehende und komplexere Projekte)

VON ANGREIFERN LERNEN

9. Verwenden Sie ein starkes Antivirusprogramm.

10. Beschränken Sie den Internetzugang auf Servern und Verwaltungscomputern. Erstellen Sie einen Terminalserver in der DMZ und benutzen Sie die Terminalbrowser-Anwendungen.

11. Verhindern Sie, dass Benutzer Skript-Programmiersprachen (vbs, js und andere) und unbekannte Dateierweiterungen ausführen können.

12. Öffnen Sie Dokumente mit Makros nur von vertrauenswürdigen Benutzern.

VON ANGREIFERN LERNEN

13. Deaktivieren Sie den Remote-Start für Powershell.

14. Zwei-Faktor-Authentifizierung (2FA / MFA) für die Netzwerkinfrastruktur einrichten, insb. um Zugriff auf Backups zu schützen.

15. Halten Sie Ihre Software auf dem neuesten Stand (Updates / Patches)!

VON ANGREIFERN LERNEN

16. Verstecken Sie offene Ports nach außen
17. Verwenden Sie komplexe Passwörter
18. Blockieren Sie den Zugriff auf den lsass-Prozess (viele Antivirenprogramme/ Security Suits tun dies)
19. Verwenden Sie das Administratorkonto nur, wenn es nötig ist
20. Schalten Sie den Computer am Ende des Tages aus
21. Sperren Sie den Computer bei Verlassen des Arbeitsplatzes

Kompetenzzentrum für Cybersicherheit in der Wirtschaft

Die Grundlagen der Digitalen Sicherheit sind nicht aufwändig in der Umsetzung, aber wirkungsvoll für den Schutz Ihrer Digitalen Daten und Wertgegenstände.

Besuchen Sie unsere Website: www.digital-sicher.nrw

Adresse

Standort Bochum
Lise-Meitner-Allee 4
44801 Bochum

Standort Bonn
Rheinwerkallee 6
53227 Bonn

Kontakt

+49 234 - 5200 7334

info@digital-sicher.nrw

Social Media

DIGITAL SICHER NRW

CYBER SECURITY CLUSTER BONN

eurobits

Beauftragt durch

Ministerium für Wirtschaft, Innovation, Digitalisierung und Energie des Landes Nordrhein-Westfalen