BILK SYSTEMHAUS

IT-Sicherheit im Handwerk

Bausteine der Sicherheit, welche Ihr Unternehmen schützen

Wer sind wir?

René Bilk

Geschäftsführer der Bilk GmbH

Sebastian Bilk

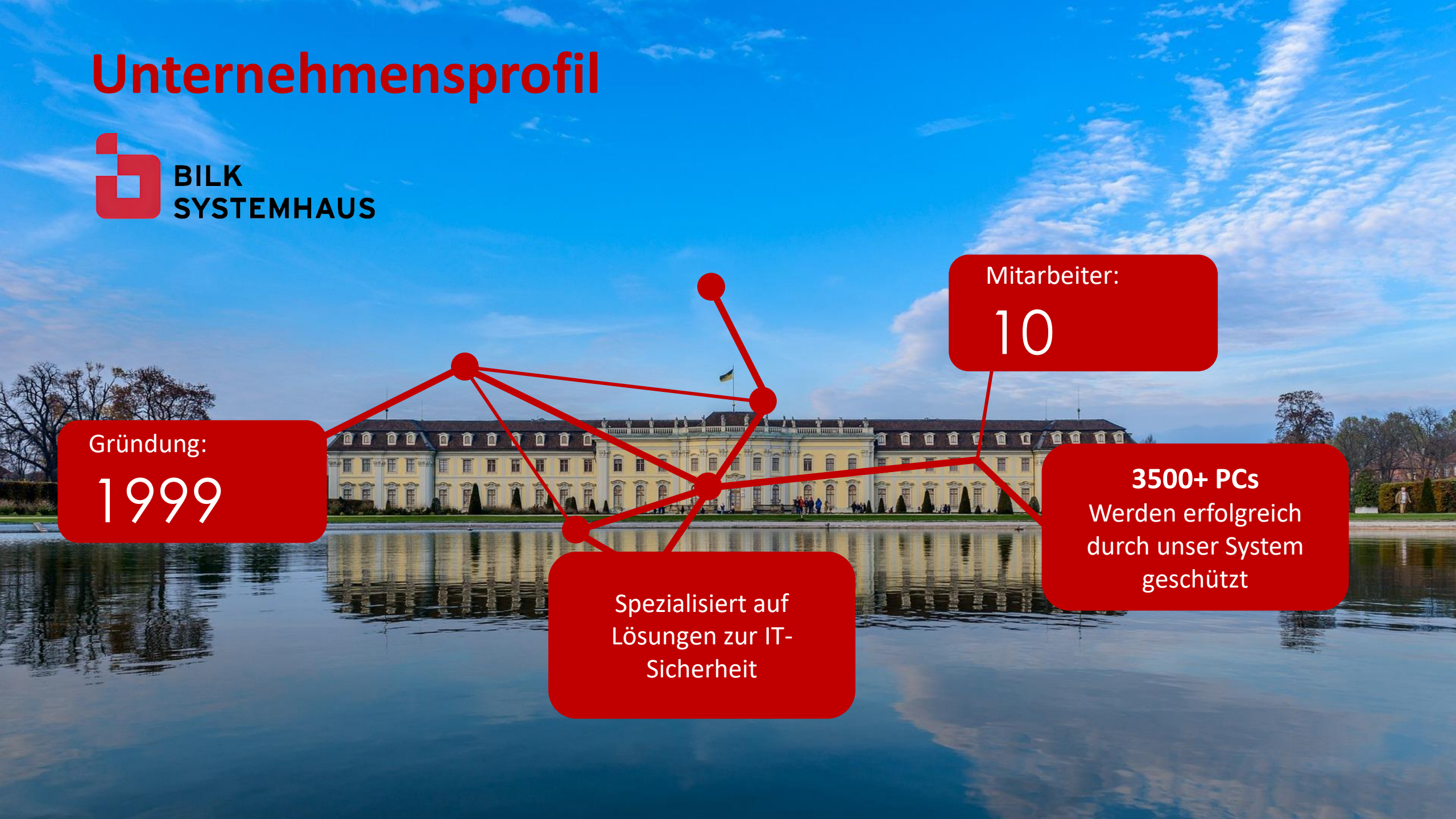
Technische Leitung der Bilk GmbH

Agenda

- Unternehmensprofil
- Wofür man IT-Sicherheit benötigt
  - Die aktuelle Bedrohungslage
  - Ransomware-Report 2023: Deutschland
  - Hacking as a Service
- Bausteine der IT-Sicherheit vorgestellt
  - Zusammenspiel Virenscanner, Firewall, Switch, AccessPoint (Synchronized Security)
  - Datenträgerverschlüsselung und Datenbackup
  - Verschlüsselte Kommunikation
  - Sicherer Datenaustausch und externer Zugriff
- Fragen

Unternehmensprofil

BILK
SYSTEMHAUS



Gründung:
1999

Mitarbeiter:
10

3500+ PCs
Werden erfolgreich durch unser System geschützt

Spezialisiert auf Lösungen zur IT-Sicherheit

BILK SYSTEMHAUS

Wofür man IT-Sicherheit benötigt

Die aktuelle Bedrohungslage

1

Microsoft durch russische Midnight Blizzard gehackt; E-Mails seit Nov. 2023 ausspioniert

Publiziert am 20. Januar 2024 von Günter Born

2

Missing Link: Ransomware-Angriffe auf Krankenhäuser gefährden Menschenleben

3

Caritas-Klinik Dominikus: Nächstes Krankenhaus kämpft mit Ransomware

Kriminelle attackieren die IT der Caritas-Klinik Dominikus in Berlin. Am Wochenende erfolgte ein Ransomware-Angriff auf die Kliniken in Mittelfranken.

4

220 Milliarden Euro Schaden durch Ransomware und andere Cyber-Angriffe

Deutsche Unternehmen beklagen zunehmende kostspielige Cyber-Angriffe. Dabei spielt Ransomware eine gewichtige Rolle.

5

"Bedrohungslage hoch wie nie": BSI warnt vor Cybercrime

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) schlägt Alarm: Das Risiko von Cyberattacken sei generell angestiegen. Auch bayerische Unternehmen waren bereits betroffen. Was lässt sich dagegen tun?

Ransomware-Report 2023: Deutschland

Sophos hat eine unabhängige Befragung von 300 IT-/Cybersecurity-Entscheidern in deutschen mittelständischen Unternehmen in Auftrag gegeben.
Die Befragung fand von Januar bis März 2023 statt.

Die Umfrageteilnehmer wurden gebeten, sich bei der Beantwortung der Fragen auf ihre Erfahrungen innerhalb des vergangenen Jahres zu beziehen.

58 % **der Befragten** waren 2023 von Ransomware betroffen.

72 % **der Angriffe** führten zur Datenverschlüsselung.
Im Vergleich zu 65% im Jahr 2022.

66 % **der Befragten** gaben an das zweite Mal in Folge Opfer eines Angriffs gewesen zu sein.

690.000 US$ **durchschnittliches Lösegeld musste von Firmen bezahlt werden.**

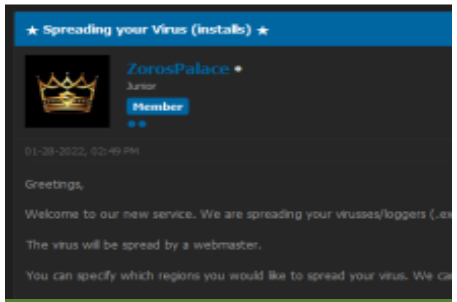
84 % **der Befragten** gaben an das Sie durch den Angriff Geschäftseinbußen oder Umsatzverluste verzeichneten.

Hacking as a Service

Access-as-a-Service

Zugriff

Verkaufen kompromittierte Accounts wie z.B. Datenbankzugriffe, Logindaten für Fernzugriff



Malware distribution / spreading-as-a-service

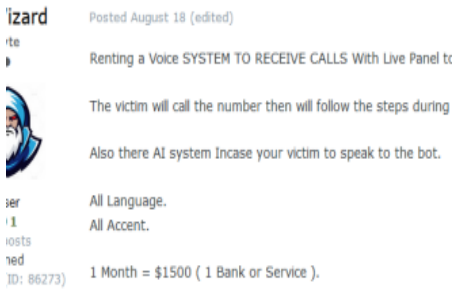
Verteilung

Erleichterung bei der Verbreitung von Schadsoftware, nach Wunsch in bestimmten Regionen oder Geschäftsbereichen

Phishing-as-a-Service

Zugangsdaten

Ende zu Ende Service für eine Phishing-Kampagne einschließlich gefälschter Webseiten, präparierter E-Mails, etc.



Vishing-as-a-Service

Social Hacking

Ende zu Ende Service für eine Vishing-Kampagne einschließlich eines KI-Systems um auf Fragen der Anrufer, ohne die Hilfe eines Menschen, zu antworten.

BILK SYSTEMHAUS

Bausteine der IT-Sicherheit vorgestellt

IT-Sicherheit veranschaulicht

Daten Backup

IT-Dokumentation

Sichere Textverabreitung

Firewall

Verschlüsselte Datenträger

Grünwald Handwerks GmbH

Antivirus System

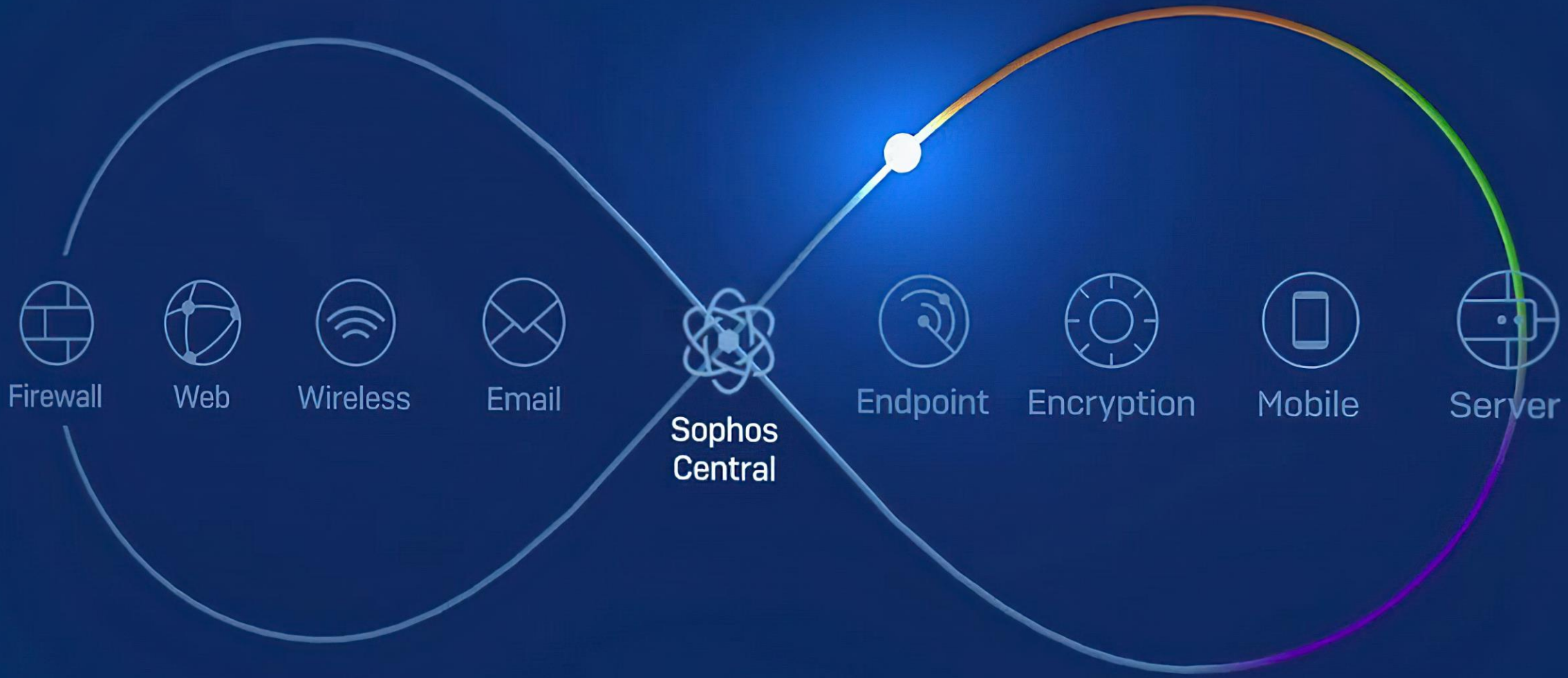
Verschlüsselte Kommunikation

Standortverbindungen mit VPN

Multifaktor Authentifizierung

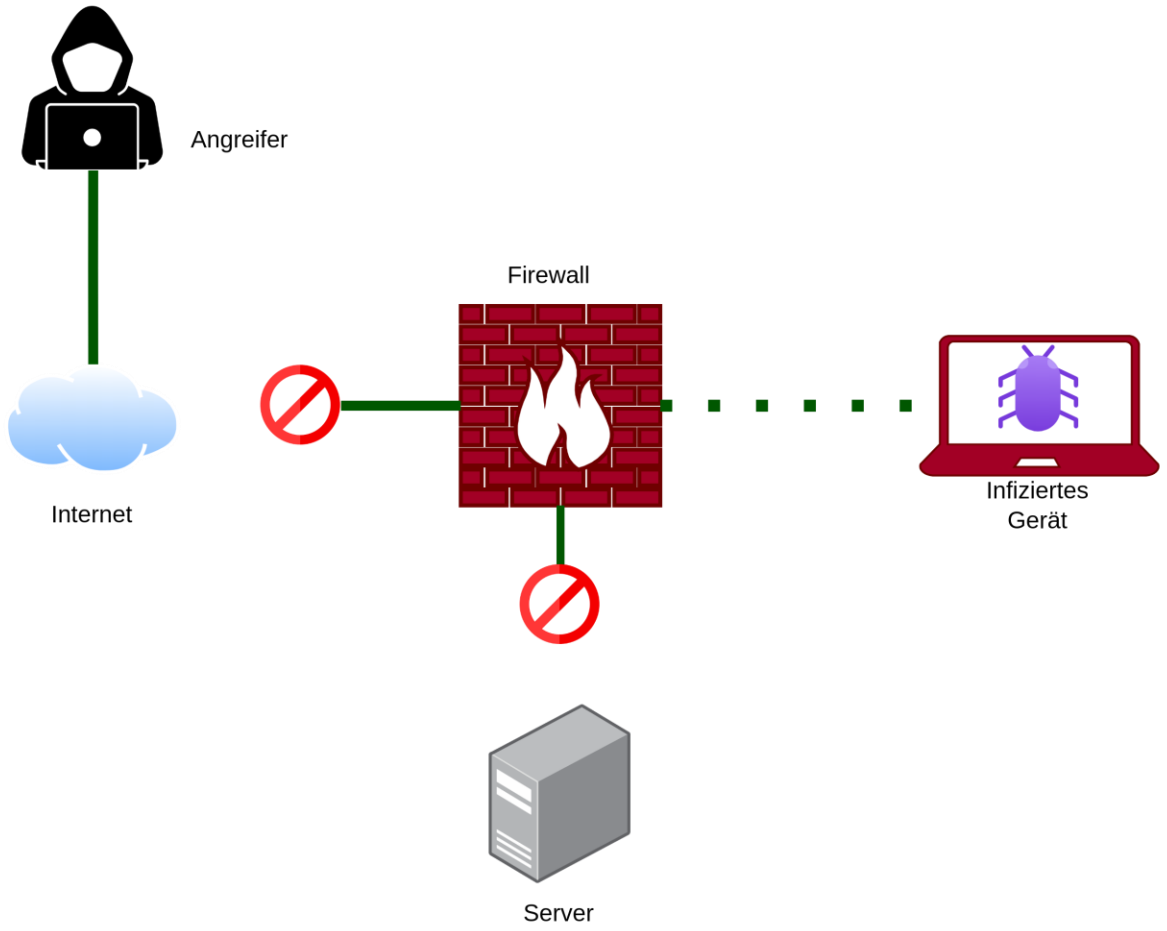
BILK SYSTEMHAUS

Zusammenspiel Virenscanner, Firewall, Switch, AccessPoint (Synchronized Security)


Firewall
Web
Wireless
Email
Sophos Central
Endpoint
Encryption
Mobile
Server

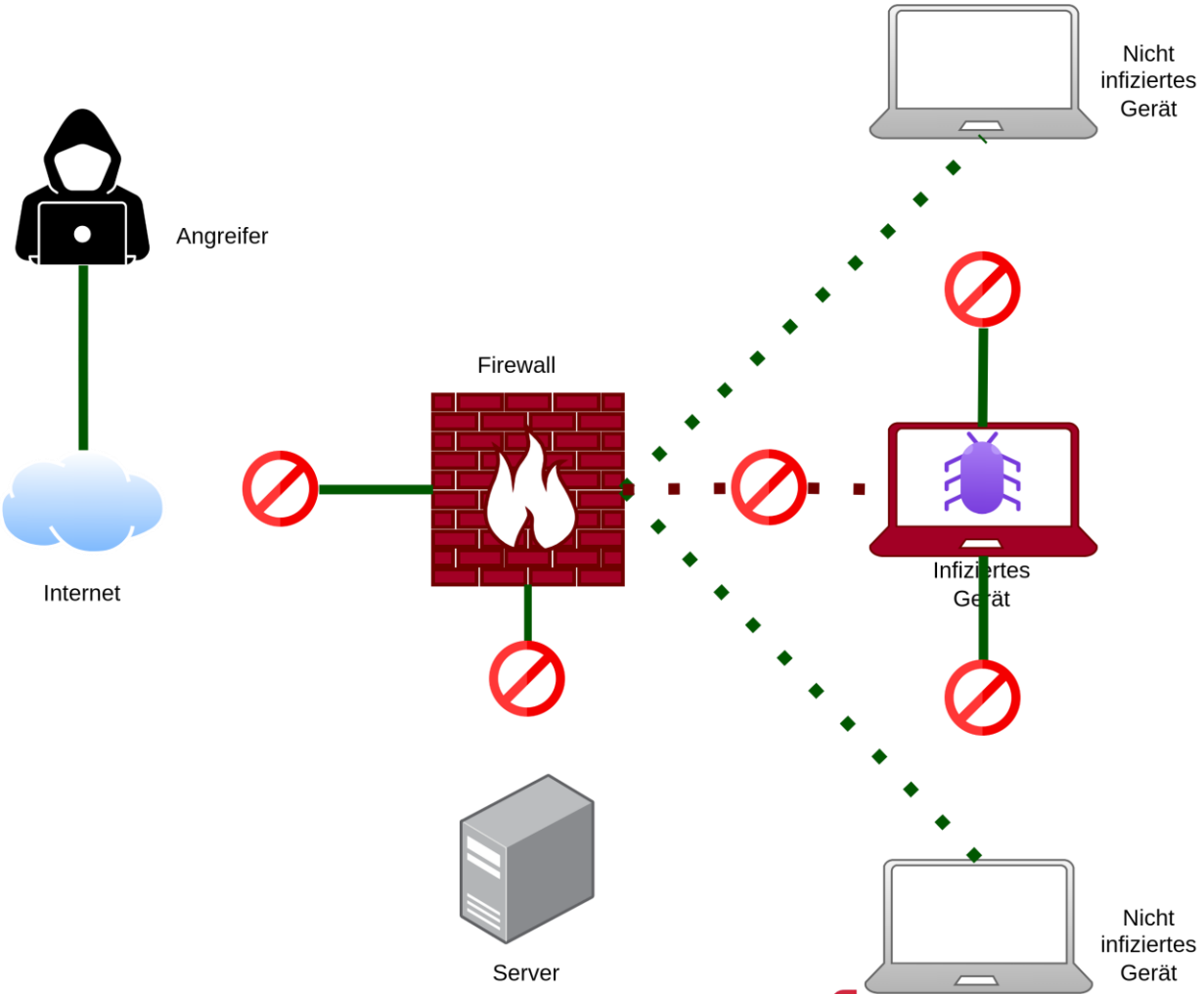
Synchronized Security in Aktion

1. Infiziertes Gerät versucht eine Verbindung zum Internet aufzubauen
2. Firewall und Antiviren Schutz erkennen die Infektion
3. Das infizierte Gerät wird für die Kommunikation mit allen internen und externen Verbindungen isoliert
4. Das infizierte Gerät wird erst nach einer Bereinigung vom System freigeschalten



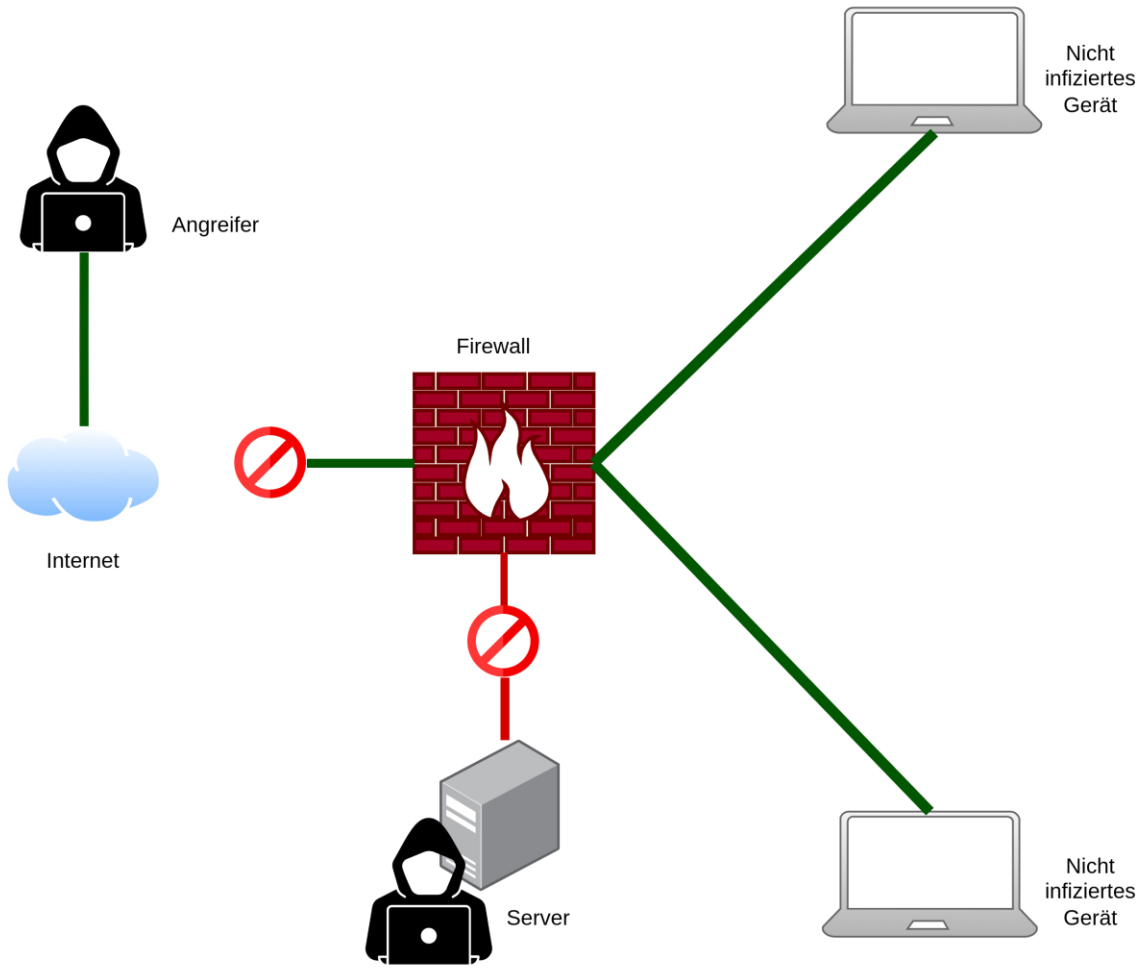
Synchronized Security in Aktion

1. Infiziertes Gerät versucht eine Verbindung zu anderen Geräten im Netzwerk aufzubauen
2. Firewall und Antiviren Schutz erkennen die Infektion
3. Das infizierte Gerät wird für die Kommunikation mit allen internen und externen Verbindungen isoliert
4. Das infizierte Gerät wird erst nach einer Bereinigung vom System freigeschalten



Synchronized Security in Aktion

1. Ein Angreifer hat sich Zugang zum System verschafft und versucht Daten zu erbeuten
2. Firewall und Antiviren Schutz erkennen ein verdächtiges Verhalten.
3. Das infizierte Gerät wird für die Kommunikation mit allen internen und externen Verbindungen isoliert
4. Das infizierte Gerät wird erst nach einer Bereinigung vom System freigeschalten



BILK SYSTEMHAUS

Datenträger Verschlüsselung und Datenbackup

Warum ich so etwas in meinem Unternehmen brauche

Datenträgerverschlüsselung: Mögliche Szenarien

1. **Einbruch in der Firma:** Sollte in Ihren Standort eingebrochen werden, können Sie sicher sein das niemand Ihre internen Daten von den Geräten auslesen kann.

2. **Laptop/ Tablet beim Kunden liegen gelassen:** Sollte es einmal passieren das ein Tablet oder Laptop beim Kunden aus Versehen liegengelassen wird, ist der Zugriff auf Ihre Daten durch die Nutzer des Gerätes beschränkt. Somit kann niemand auf die sensiblen Kundendaten zugreifen.

3. **Einbruch ins Fahrzeug:** Durch die Verschlüsselung der Daten ist das Notebook für den Dieb nutzlos und Sie brauchen sich keine Sorgen über einen Datenschutzverstoß machen.

Datenbackup: Mögliche Szenarien

1

Ransomware Attacke: Durch eine Ransomware Attacke, werden alle Ihre Daten auf den Servern und Geräten verschlüsselt. Durch ein Datenbackup können Sie diese Daten wiederherstellen, ohne ein Lösegeld zu bezahlen.

Durchschnittlicher Preis für Lösegeldzahlung:

690.000 US$

Durchschnittlicher Preis für Datenwiederherstellung durch Backups:

375.000 US$

Datenbackup: Mögliche Szenarien

2 **Einbruch in die Firma:** Sollte es einmal passieren, das jemand in Ihre Firma einbricht und Ihre Geräte und Server stehlen sollte, können Sie Ihr letztes Datenbackup einspielen, mit geringer Unterbrechung Ihre wertvollen Geschäftsdaten wiederherstellen und den Firmenbetrieb schnell wieder aufnehmen.

3 **Menschliche Fehler:** Sollten durch einen Fehler, wichtige Dokumente oder Daten gelöscht worden sein. Können Daten durch ein Datenbackup wiederhergestellt werden. Das gleiche gilt, sollte es zur Korruption von Daten durch das Abspeichern kommen.

4 **Höhere Gewalt:** Eine Naturkatastrophe wie Überschwemmungen, Erdbeben oder Brände beschädigt die physische Infrastruktur Ihres Unternehmens.

BILK SYSTEMHAUS

Sichere Kommunikation im Unternehmen

Möglichkeiten der sicheren Kommunikation

1. **Sicherer Messenger:** Messenger wie Signal um die Kommunikation zwischen Ihnen und Ihrem Gesprächspartner verschlüsselt zu übertragen

2. **Verschlüsselung der E-Mail-Kommunikation:** Verschlüsseln Sie Ihre E-Mail-Kommunikation mit Personen innerhalb und Außerhalb ihres Unternehmens, damit Dritte keine Einsicht in Ihre Unterhaltung haben.

3. **Signieren Sie Ihre E-Mail-Kommunikation:** Mit dieser Maßnahme ist es für Angreifer schwieriger sich als Sie auszugeben und Ihr gegenüber weiß das Sie es wirklich sind.

Vorteile eines Messenger Dienstes wie Signal

1. **Sicherer Messenger:** Messenger wie Signal verschlüsseln die Kommunikation beider Parteien ohne Daten an einen dritten Anbieter weiterzugeben.

2. **Signal speichert keine Daten:** Die einzige Information, welche der Signal Messenger von Ihnen speichert ist Ihre Telefonnummer als ein Accountname. Das macht Signal, Datenschutz unbedenklich für die Kommunikation.

3. **Kein Tracking und benutzerdefinierte Werbung:** Durch den Status einer Stiftung ist Signal durch Spenden finanziert und dadurch Unabhängig.

4. **Signal ist kostenlos:** Die Signal App kann kostenlos installiert werden und somit ist auch die sichere Kommunikation über Signal kostenlos.

Vorteile eines Messenger Dienstes wie Signal

Daten, welche der Signal Messenger von Ihnen besitzt

Attachment A

Account	Information
+[redacted]	N/A
+[redacted]	Last connection date: 1454198400000 Unix millis Account created: 1453475222063 Unix millis

Daten, welche andere Messenger von Ihnen besitzen

- Informationen zu Ihrem Konto
- Ihre Kontakte
- Informationen über Ihre Gemeinschaft und Gruppen
- Informationen zum Kundensupport und andere Mitteilungen
- Protokoll und Informationen zur Fehlerbehebung
- Geräte- und Verbindungsinformationen
- Informationen zur Nutzung
- Allgemeine Standortinformationen
- Benutzerberichte

BILK SYSTEMHAUS

Sicherer Datenaustausch und externer Zugriff

Möglichkeiten des sicheren Datenaustauschs

1. **Zugriff über einen verschlüsselten Zugang:** Greifen Sie durch einen sicheren Zugang mit ZTNA oder VPN auf Daten innerhalb Ihres Netzwerks zu und verbinden Sie somit mehrere Standorte miteinander.

2. **Versenden von passwortgeschützten Links:** Durch das Versenden von Passwortgeschützten Links ist es möglich, unbefugten den Zugriff auf Dateien schwer zu machen. Optional kann sogar ein Ablaufdatum für den Link gesetzt werden damit dieser nach einer festgelegten Zeit nicht mehr aufrufbar ist.

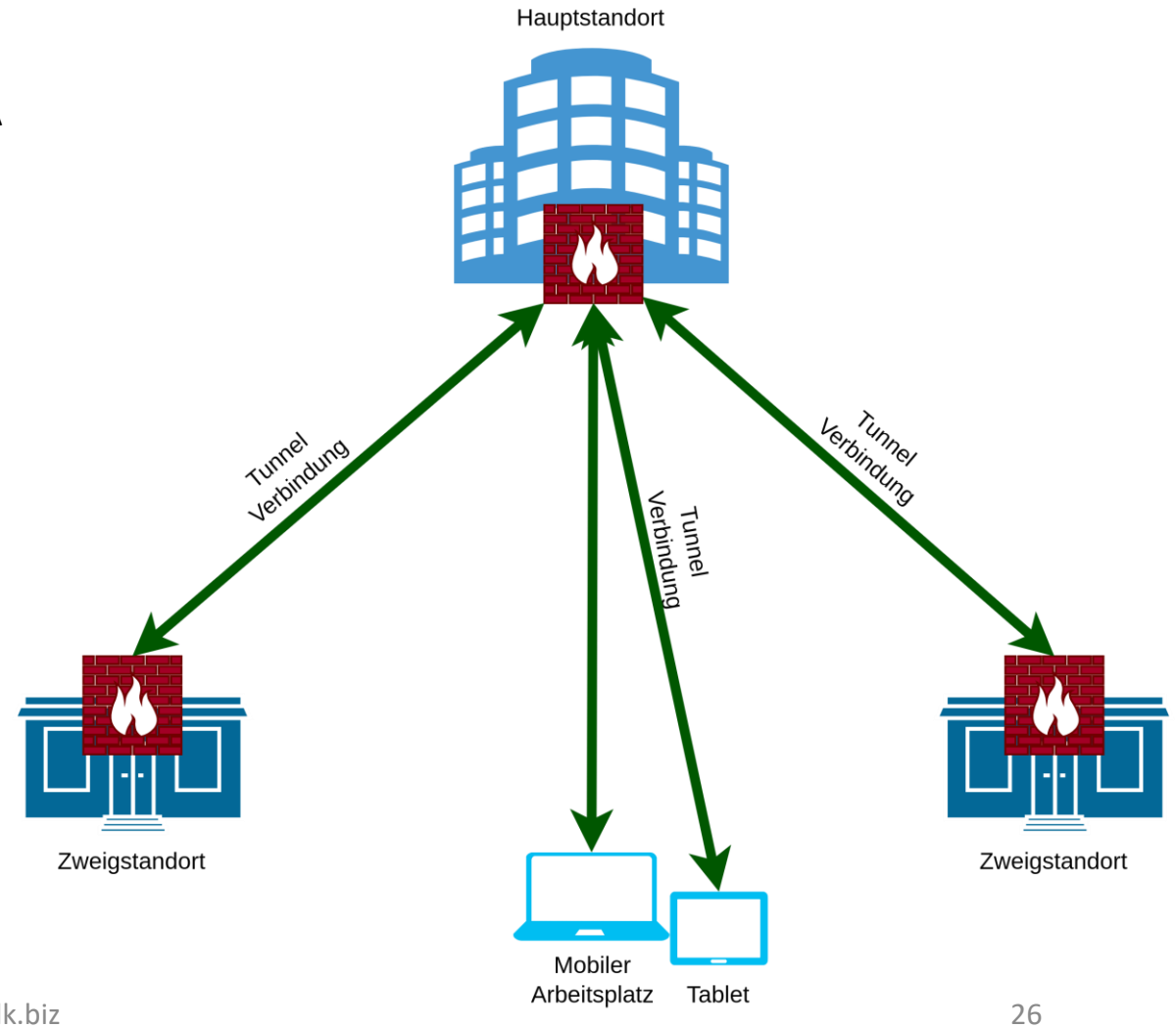
3. **Beschränken Sie den Zugriff auf Daten:** Durch die Beschränkung von Zugriffen für einen bestimmten Personenkreis ist es unbefugten Personen nicht möglich auf diese Dateien zuzugreifen. Dadurch bleiben Ihre Daten sicher und geraten nicht in falsche Hände.

4. **Verschlüsseln von Dokumenten beim Versenden über E-Mail:** Verschlüsseln Sie Dokumente mit einem zuvor abgesprochenen Passwort, damit beim versandt an den falschen Empfänger es nicht geöffnet werden kann.

Möglichkeiten des Zugriffs von Außerhalb

1. **Zugriff über einen verschlüsselten Zugang:** Greifen Sie durch einen sicheren Zugang mit ZTNA oder VPN auf Daten innerhalb Ihres Netzwerks zu und verbinden Sie somit mehrere Standorte miteinander.

2. **Nutzen Sie für den Austausch von Daten zwischen Baustelle mit dem Büro einen Cloudservice:** Speichern Sie Daten in der Cloud um von der Baustelle, vom Büro oder von Zuhause, Zugriff auf Ihre Daten zu haben.



Fragen:

Das-Handwerk-Digital.de
BRANCHENORIENTIERTE DIGITALBERATUNG

BILK SYSTEMHAUS

Vielen Dank für Ihre Aufmerksamkeit!