
Leipzig, 19.05.2016

Liebe Leserinnen und Leser,

Schlagzeilen über Cyber-Angriffe sind eine Erinnerung daran, dass IT-Bedrohungen stetig wachsen und Unternehmen jeder Größe beim Einsatz digitaler Technologien und dem Internet täglich mit signifikanten Risiken zu kämpfen haben. Die meisten Unternehmen setzen umfangreiche Sicherheitsmechanismen wie Virenscanner, Firewalls, IPS-Systeme, Anti-SPAM/ Antiviren-Email-Gateways und Webfilter ein. Dennoch werden weltweit Infektionen von Rechnern mit Verschlüsselungstrojanern wie Cryptowall, TeslaCrypt oder Locky, registriert. Sie verschlüsseln Dateien auf Rechnern und Netzlaufwerken, mit dem Ziel, von den Nutzern für das Entschlüsselungswerkzeug Geldbeträge von mehreren hundert US-Dollar (200 – 500) zu erpressen.

Wie kann sich Ihr Unternehmen vor elektronischen Erpressungen schützen? In dieser Ausgabe unseres eMagazins beschäftigen wir uns ausführlich mit dem Thema **Endpoint Security.** Wir wünschen Ihnen viel Spaß beim Lesen!

## Warum ist es heute wichtig auf Endpoint-Schutz zu setzen?

Sicherheitsanbieter haben erhebliche Anstrengungen unternommen, um Cyberbedrohungen zu neutralisieren. Die heutige Sicherheitssoftware setzt auf eine Kombination zahlreicher Schutzebenen, die zur Abwehr moderner Bedrohungen und zur Sicherung sensibler Daten auf Laptops und PCs unerlässlich sind. Endpoint-Schutz ergänzt netzwerkbasierte Sicherungsvorkehrungen, indem dafür gesorgt wird, dass Computer und Geräte vor Malware und Datenverlusten bewahrt werden.

| Anti-Virus 1.0 | Anti-Virus 2.0 | Endpoint Security 1.0 | Endpoint Security 2.0 |
|---|---|---|---|
| Schutz gering | >> | >> | Schutz hoch |
| • Kennungs-basierter Virenschutz | • Kennungsbasierter Virenschutz<br>• Host Intrusion Prevention Systeme (HIPS) | • Kennungsbasierter Virenschutz<br>• Client Firewall<br>• Erkennung verdächtiger Dateien/ Verhaltensmuster<br>• Application Control<br>• Device Control | • Kennungsbasierter Virenschutz<br>• Live „In-the-Cloud“ Antiviren-Checks<br>• Standortspezifische Client Firewall<br>• Erkennung verdächtiger Dateien und Verhaltensmuster<br>• Application Control<br>• URL-Filterung<br>• Device Control |

| | | | |
|---|---|---|---|
| | | | • Datenverschlüsselung<br>• Data Loss Prevention (DLP)<br>• Single Agent<br>• Eine Management-Konsole für alle Plattformen |

Heutzutage gibt es Szenarien bei denen herkömmliche Anti-Virus-Programme an ihre Grenzen stoßen und somit keinen ausreichenden Schutz mehr bieten:

- Zero-Day-Bedrohungen
- Arbeiten im Internet ohne Firewall und Webschutz/ Drive by Downloads
- Sicherheitslücken durch ungepatchte PCs

## Softline Services

Wir stellen Ihre Endpoint Security auf den Prüfstand, beraten Sie zum Thema Maleware Defense und entwickeln mit Ihnen Ihre Sicherheitsstrategie weiter. Die Softline Solutions bietet Ihnen folgende Services an:

- ✓ **Sicherheits-Assessment** (Fokus Antivirenschutzmaßnahmen)
- ✓ **Endpoint Protection as a Service** (Managed Security Service)
- ✓ **Erarbeitung von Sicherheitsstrategien/ -konzepten**

Können wir Sie in diesen Bereichen unterstützen? Dann kontaktieren Sie uns gerne unter it-sicherheit@softline-group.com oder +49 341 24051-0.

## Daten als Geisel

### Ransomware

Kryptotrojaner oder »Cyberterroristen« sind Schadprogramme durch die eine Zugriffs- oder Nutzungsverhinderung von Daten sowie des gesamten Computersystems bewirkt werden. Sie verschlüsseln Daten auf einem fremden Computersystem und auf im Zugriff befindlichen Netzwerkressourcen oder verhindern den Zugriff auf diese. Für die Entschlüsselung bzw. Freigabe der Daten wird ein »Lösegeld« gefordert.

**10 Regeln, die vor elektronischer Erpressung schützen**:

1. **Vor dem Öffnen einer E-Mail immer wachsam sein!**

   E-Mails zu fälschen und dadurch einen vertrauten Eindruck zu erwecken, ist relativ einfach.

2. **Bei der Ausführung von Mail-Anhängen misstrauisch sein!**

   E-Mail-Anhänge nur öffnen, wenn man dem Absender vertraut. Besondere Vorsicht ist geboten bei der Ausführung von Programmcodes, wie z. B. JavaScript *.js, *.exe, *.bat, *.com, *.vbs, *.ps und bei gepackten Dateien wie etwa ZIP oder RAR.

3. **Niemals Links direkt in E-Mails anklicken!**

   Es ist schwer zu erkennen, wohin ein Link tatsächlich führt. Daher sollten Links in E-Mails **nie** angeklickt werden. Es ist technisch sehr leicht realisierbar einen Link so aussehen zu lassen, als würde er zu einer vertrauenswürdigen Stelle führen, obwohl er auf eine manipulierte Seite zum Herunterladen von Schadsoftware (Drive-by Download) oder zum Abfangen von Zugangsdaten (Phising) führt.

4. **Spam-Nachrichten auch als »Spam« markieren!**

   Wird eine Spam-Nachricht nicht erkannt, sollte diese als Spam markiert und in den Spam-Ordner verschoben werden, oder als solche markiert und erst anschließend gelöscht werden.

5. **E-Mail-Adressen nicht arglos im Netz veröffentlichen!**

Im Internet veröffentlichte E-Mail-Adressen werden gezielt und automatisiert gesucht, um an diese Spam zu senden. Deshalb sollten sie nicht unbekümmert auf der Webseite veröffentlicht werden.

6. **Daten sichern!**

   Regelmäßige Backups von Daten und Systemen sollten zur Selbstverständlichkeit gehören. Es ist wichtig kontinuierlich zu prüfen, ob sich die gesicherten Daten auch tatsächlich wiederherstellen lassen.

7. **Immer »up to date« sein!**

   Ein großes Sicherheitsrisiko liegt in ungepatchten Systemen: Betriebssystem, Internet-Browser, Plug-Ins, Antiviren/ HIPS/ Spam Programme und Anwendungen sollten immer aktuell sein. Nicht gepatchte Systeme stellen ein großes Einfallstor für Schädlinge dar.

8. **Automatisches Ausführen von Makros und Applikationen stoppen!**

   »Locky« befällt bis dato vor allem Windows-Rechner, auch andere Betriebssysteme können gefährdet sein. Wichtig ist, die Systeme so zu härten, auch Office-Anwendungen so zu konfigurieren, dass der Makro-Code nicht oder erst nach einer Rückfrage ausgeführt wird.

9. **Externe Datenspeicher nicht fest am Rechner belassen!**

   »Viele Verschlüsselungs-Trojaner können auch Daten auf externen Laufwerken und Netzlaufwerken unbrauchbar machen«, heißt es beim Bundesamt für Sicherheit in der Informationstechnik. Dort empfiehlt man: »Verbinden Sie deshalb das Speichermedium für Ihre Datensicherungen nicht dauerhaft mit Ihrem Computer.«

10. **Den Notfallplan in der Tasche haben!**

    Der **wichtigste Punkt** ist, einen **Plan für den Ernstfall** zu erarbeiten.

    - Wie erkenne ich überhaupt eine Gefährdung?
    - Wie verhalte ich mich im Notfall, um größeren Schaden zu vermeiden?

## Prüfen Sie ihre eigene IT-Sicherheit! Beantworten Sie dazu folgende Fragen:

- Wie schützen Sie Ihre Systeme vor schädlichen Websites, wenn Ihre Mitarbeiter außerhalb des Büros im Internet surfen?
- Wie besorgt sind Sie über Sicherheitslücken zwischen Updates Ihres Sicherheitsanbieters?
- Wie halten Sie Ihren Schutz unternehmensweit auf dem neuesten Stand?
- Wie viele Ihrer Nutzer haben nicht zugelassene Anwendungen, wie z. B. VoIP, IM, P2P und Spiele installiert?
- Wie unterbinden Sie, dass Mitarbeiter vertrauliche Unternehmensdaten auf Wechselmedien speichern?
- Können Sie alle, sich mit Ihrem Netzwerk verbindenden Computer, auf die Aktivierung von Virenschutz, einer Firewall und Windows Updates überprüfen?

Benötigen Sie Hilfe bei der Auswertung?
Dann wenden Sie sich gerne an unseren IT-Sicherheitsexperten Ulf Seifert.

## Was sind die Bestandteile einer State of The Art Endpoint Security Lösung?

**Virusscan:** Er bildet die Grundlage für eine geschützte IT-Struktur. Auch wenn viele Virenscanner einen umfangreichen Schutz bieten, stellen sie kein Sicherheitsallheilmittel dar und sollten daher mit anderen Sicherheitsprodukten kombiniert werden.

**Applikationskontrolle:** Sie unterstützt bei der Erstellung einer Whitelist mit erlaubter Software, die auf dem Endgerät ausgeführt werden darf. Software, die über USB-Sticks oder das Netzwerk eingeschleust wird, kann somit nicht ausgeführt werden.

**Änderungskontrolle:** Im laufenden Betrieb erfolgen innerhalb der IT-Struktur viele Anpassungen, Änderungen und Erweiterungen von Betriebssystemen und Softwareapplikationen. Mit Hilfe einer Software zur Änderungskontrolle werden diese Veränderungen freigegeben oder blockiert. Dabei werden nicht autorisierte Veränderungen an Systemdateien, Verzeichnissen und Konfigurationseinstellungen verhindert.

**Device Control:** Oft wird Schadsoftware unbewusst durch die unbedachte Verwendung von (auch privaten) Wechseldatenträgern auf Geräte in das Firmennetzwerk eingeschleust. Über Device Control wird genau das verhindert, in dem Schnittstellen von Computersystemen überwacht oder blockiert werden (z. B. USB-Laufwerke oder beschreibbare CDs).

**Host Intrusion Protection Systeme:** Anders als der Schutz vor Viren und Schadcode bietet das HIPS Modul (Host Intrusion & Protection System) eine umfassende Verteidigung des Betriebssystems. Die Überwachung erfolgt auf Grundlage bekannter Signaturen, wird jedoch auch durch Verhaltensanalyse unterstützt.

**Sandbox:** Mit dem Begriff Sandbox wird eine Technik bezeichnet, Software innerhalb einer speziellen – d. h. von den übrigen Systemressourcen isolierten – Laufzeitumgebung auszuführen. Die Technik kann mit dem Prinzip von in sich geschlossenen Containern verglichen werden, in denen Software ausgeführt wird, ohne andere Ressourcen eines Systems zu beeinflussen.

**Personal (Client) Firewall:** Ist eine hostbasierte Firewall zum Schutz des lokalen Computers, die den Datenaustausch des Computers mit verschiedenen Netzwerken bzw. dem Internet überwacht und einschränkt.

## Gesetze und Normen

Seit Mitte 2012 ist das Bundesdatenschutzgesetz (BDSG) für jedes Unternehmen in vollem Umfang wirksam. Alle Organisationen können »anlassfrei« geprüft werden. Eine Prüfung steht an, wenn ein Anlass vorliegt – also beispielsweise eine Beschwerde eines Betroffenen bei der Aufsichtsbehörde eingeht. Die Behörde würde in diesem Fall das Datenschutzniveau des Unternehmens mit den Bestimmungen des BDSG abgleichen müssen und ggf. Nachbesserungen und Bußgelder fordern.

### TECHNISCHE MASSNAHMEN LAUT BDSG:

- Im Paragraph 9 Satz 1 gibt es die Punkte 1 bis 8, die ganz konkret technische Maßnahmen der Datenverarbeitung regeln.
- Im Punkt 3 des Paragraphen wird eine Zugriffskontrolle gefordert.
- Der Punkt 4 regelt die Gewährleistung, dass personenbezogene Daten nicht von Unbefugten gelesen werden können. Hierzu wird explizit eine Verschlüsselung nach dem Stand der Technik gefordert.
- Der Punkt 5 regelt die Protokollierung, denn es muss im Schadensfall nachträglich überprüft werden können, ob, von wem und in welchem Umfang auf personenbezogene Daten zugegriffen wurde.
- Punkt 7 besagt, dass personenbezogene Daten gegen Zerstörung, Verlust und auch Schadsoftware (Malware) geschützt werden müssen.

Wichtig sind weiterhin §§ 4b Abs. 2 und 4c BDSG, die die Nutzung von Cloud-Diensten betreffen.

## Rahmenbedingungen für Implementierung und Betrieb von Endpoint Security

**Technische Rahmenbedingungen:**

- Prüfen Sie regelmäßig die Konformität Ihrer Maleware Schutzprogramme. Diese müssen sicher, wirkungsvoll und entsprechend Ihrer Sicherheitsvorgaben bzw. Best Practices konfiguriert sein!
- Prüfen Sie die Aktualität Ihrer IT Infrastruktur. Diese ist ebenso entscheidend für die Sicherheit ihrer IT-Umgebung.
- Minimieren Sie Anwenderrechte an Systemen, und vergeben Sie Schreibrechte sparsam.

**Organisatorische Rahmenbedingungen:**

- Erarbeiten Sie ein Sicherheitskonzept für Ihre Organisation. Geben Sie im Konzept entsprechende Schutzmaßnahmen für die Peripherie vor.
- Benennen Sie Fachpersonal als zentrale Ansprechpartner bei Fragen rund um das Thema Schadsoftware!
- Schulen und sensibilisieren Sie regelmäßig alle Mitarbeiter zum Thema IT-Sicherheit!

Wir beraten Sie gern allumfassend zur Einführung technischer und organisatorischer Maßnahmen im Zusammenhang mit Endpoint Security. Informationen zu den Security@Softline Workshops finden Sie auf unserer Webseite.

## vShield Endpoint // AV-Schutz in einer virtualisierten Umgebung

### Warum vShield Endpoint?

Unternehmen schützen ihre virtuellen Systeme oft auf klassische Art und Weise – also wie einen normalen Client – mit einer Endpoint-Sicherheitslösung. In virtualisierten Umgebungen stößt diese Variante jedoch schnell an ihre Grenzen. Wo die klassische Lösung nicht weiterhilft und welche Vorteile agentenlose virtuelle Systeme bieten, erfahren Sie in unserem Unternehmens-Blog.

## Sonstiges

**Breaking News:**

- MS Patchday 12.4. u. a. mit IE/ EDGE Updates um Lücken zu schließen, welche Schadcode in den Computer einschleusen und Benutzerrechte erlangen könnten.
- Adobe Updates dienen u. a. zum Schließen von Sicherheitslücken, welche von Ransomware wie Locky ausgenutzt werden.
- WhatsApp verschlüsselt nur Nachrichten, nicht Metadaten wie Adressbuch oder Übertragungszeitpunkt und Empfänger.
- Erste Tools berechnen anhand verschlüsselter Daten den Schlüssel von Erpressungs-Trojanern wie Petya.
- Bundestrojaner 2.0 bietet aufgrund der alleinigen Unterstützung auf PCs nicht den gewünschten Nutzen. Keine Unterstützung für Tablets, Smartphones, MACs oder Linux basierende Geräte.

---

**Sophos Sandstorm:**

Neue Lösung zur Abwehr von Advanced Persistent Threats (APT) und Zero-Day Malware. Durch Einsatz leistungsstarker cloudbasierter Next-Generation-Sandbox-Technologie ermöglicht z. B. Sophos Sandstorm eine schnelle und zuverlässige Erkennung, Blockierung und Reaktion auf evasive Malware

**CylancePROTECT**:

Neue Cybersecurity-Lösung: künstliche Intelligenz gegen Maleware. Diese Lösung verzichtet bei der Abwehr von Bedrohungen komplett auf klassische Signaturen. Die Software analysiert

---

die »DNA« des Codes vor der Ausführung auf dem Endpoint, um Bedrohungen zu finden und zu verhindern

---

**Veranstaltungshinweise:**

- **Security Business Frühstück: »Digitale Erpressung – Wie lässt sich die Geiselnahme von Daten verhindern?«**
  10. Juni 2016 in Leipzig
  *Im fachlichen Fokus der Vorträge steht die Auseinandersetzung mit der Bedrohungslage durch Verschlüsselungstrojaner wie Locky & Co. Welche Maßnahmen müssen Unternehmen ergreifen, um eine Geiselnahme ihrer Daten zu verhindern? Welche Rolle spielt hierbei die Endpoint Security? In einer moderierten Diskussionsrunde können sich Geschäftsführer, leitende Angestellte und IT-Verantwortliche zudem über Maßnahmen gegen bösartige Schadsoftware austauschen.*
  **>>** Zur Anmeldung

- **protekt – Konferenz und Fachausstellung für den Schutz kritischer Infrastrukturen**
  22. bis 23. Juni 2016 in Leipzig **>>** Weitere Informationen

---

Falls Sie Fragen oder Hinweise zu gewünschten Magazininhalten haben oder unsere Unterstützung in IT-Sicherheitsprojekten benötigen, dann kontaktieren Sie uns unter it-sicherheit@softline-group.com oder telefonisch unter +49 341 24051-0.

Mit freundlichen Grüßen

Ihr Softline Team.

Softline Solutions GmbH // Geschäftsführer: Martin Schaletzky // Sitz der Gesellschaft: Leipzig // Handelsregister Leipzig: HRB 26058 // Steuer Nr.: 232/118/06001 // USt ID: DE270894910