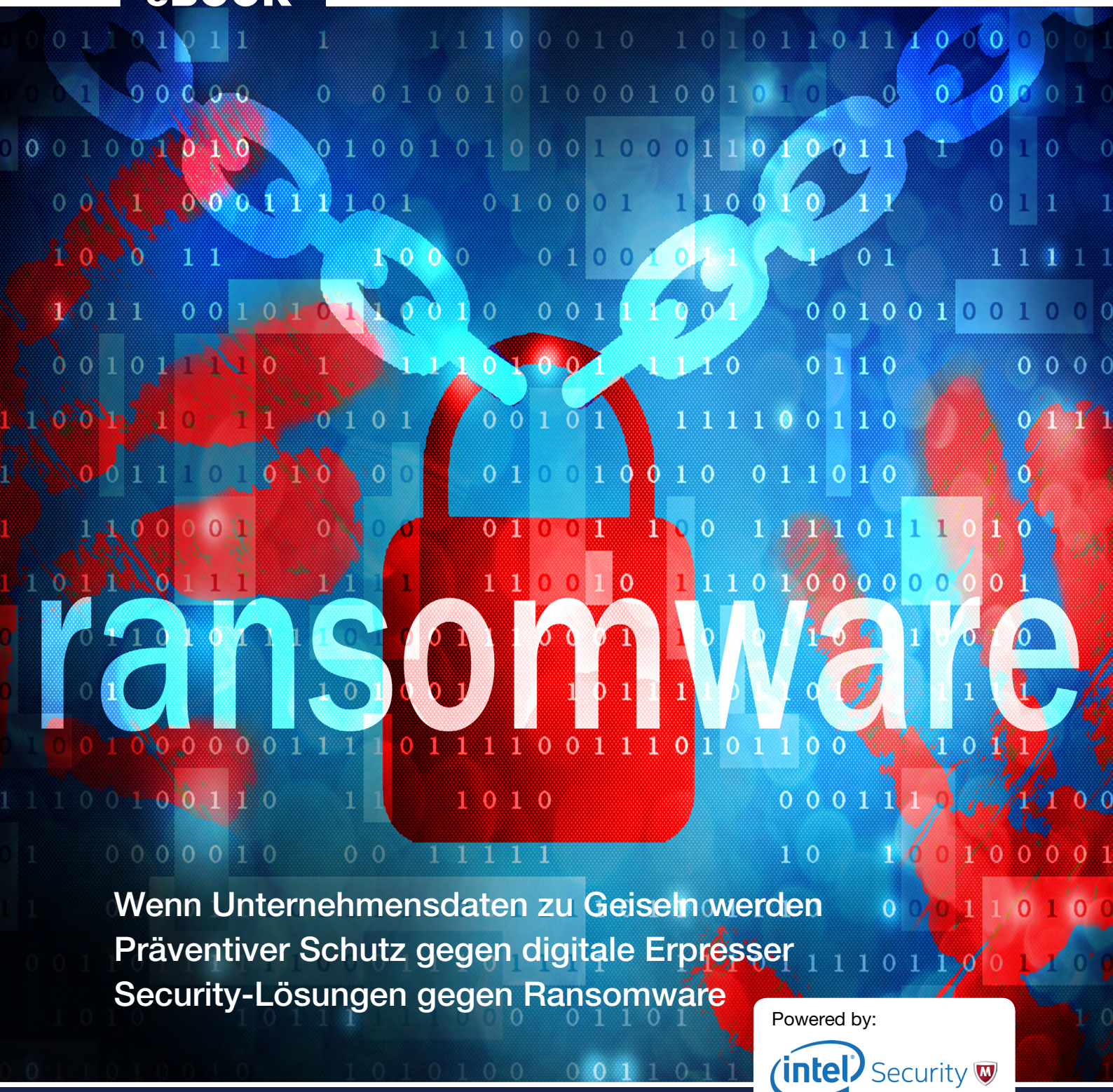
www.Security-Insider.de

Eine Publikation von:
Security Insider

Ransomware

eBOOK



Wenn Unternehmensdaten zu Geiseln werden
Präventiver Schutz gegen digitale Erpresser
Security-Lösungen gegen Ransomware

Powered by:
intel Security
McAfee is now part of Intel Security.

Vogel Business Media

Inhalt

Powered by: intel Security

McAfee is now part of Intel Security.

Intel Deutschland GmbH
Ohmstr. 1, 85716 Unterschleißheim
Telefon +49 (0)89 37 07-0
E-Mail Info_Deutschland@McAfee.com
Web www.mcafee.com/de

Vogel IT-Medien GmbH
August-Wessels-Str. 27, 86156 Augsburg
Telefon +49 (0) 821/2177-0
E-Mail redaktion@security-insider.de
Web www.Security-Insider.de
Geschäftsführer: Werner Nieberle
Chefredakteur: Peter Schmitz, V.i.S.d.P., peter.schmitz@vogel-it.de
Erscheinungstermin: Dezember 2015
Titelbild: santiago silver - Fotolia.com

Wenn Daten zu Geiseln werden

Schadsoftware kann die Daten betroffener Unternehmen nicht nur ausspähen, löschen oder inhaltlich manipulieren. Spezielle Formen von Malware, sogenannte Ransomware, können die Daten auch verschlüsseln und Lösegeld für eine Entschlüsselung erpressen.

Ransomware ist ein lukratives, kriminelles Geschäft, wie die Statistiken der Cyber Threat Alliance zur CryptoWall-Attacke zeigen. Deshalb sind weitere Angriffe wahrscheinlich, eine Prävention sehr zu empfehlen. (Bild: cyberthreatalliance.org)

Angebliche Bewerber können gefährliche Erpresser sein

Die E-Mail-Bewerbung macht einen ganz normalen Eindruck. Der Empfänger in der Personalabteilung öffnet die Mail, die in der Betreffzeile auf eine ausgeschriebene Stelle referenziert. Neben einem kurzen Anschreiben enthält die Bewerbungsmail noch einen PDF-Anhang. Der Lebenslauf, der in der PDF-Datei zu finden ist, wird laut Angaben des Bewerbers noch um weitere Dokumente ergänzt, die nicht mitgeschickt wurden, sondern zum Download auf einem Dropbox-Konto bereitliegen.

Wenn nun die Mitarbeiterin oder der Mitarbeiter der Personalabteilung die weiteren Anhänge aus der Cloud abrufen möchte, wird aus der scheinbaren Bewerbung plötzlich eine Online-Attacke: Über den Link im PDF-Dokument wird der sogenannte Chimera-Trojaner heruntergeladen. Dieser Trojaner gehört zur Familie der Ransomware. Die Schadfunktion besteht darin, dass die Daten auf dem Rechner des Opfers verschlüsselt werden. Nur wenn das betroffene Unternehmen eine bestimmte Summe Geld überweist, sollen die Daten wieder entschlüsselt werden. Geschieht dies nicht, bleiben die Daten für das Unternehmen nicht nur verschlüsselt und damit unzugänglich. Die sich öffnende Meldung des Trojaners droht sogar damit, die vertraulichen Daten zu veröffentlichen, wenn kein Geld fließen sollte.

Ransomware zieht immer weitere Kreise

Die zuvor beschriebenen Angriffe auf Personalabteilungen sind keine Einzelfälle. Attacken mit Ransomware und damit Erpressungsversuche über das Internet finden in vielen Bereichen statt und sind seit Jahren eine Bedrohung. Die Zahl der Ransomware-Attacken nimmt allerdings immer mehr zu, wird immer raffinierter und betrifft auch zum Beispiel Daten, die auf mobilen Endgeräten vorgehalten werden.

So berichtete der Verband der Internetwirtschaft eco davon, dass Ransomware zunehmend die Oberflächen mobiler Endgeräte sperrt und erst nach Zahlung eines Lösegelds wieder freigeben will. Das Anti-Botnet-Beratungszentrum von eco berichtet auch von einem sogenannten „BKA-Trojaner“, der besonders Nutzer von Android-Smartphones betrifft. Bei dieser Form der Attacke werden die mobilen Endgeräte angeblich vom Bundeskriminalamt

Ransomware: Verschlüsselung wider Willen

Top Threats	Current Trends	Top 10 Threat Trends in Emerging Areas						
		Cyber-Physical Systems and CIP	Mobile Computing	Cloud Computing	Trust Infrastr.	Big Data	Internet of Things	Netw. Virtualisation
1. Malicious code: Worms/Trojans	↑	↑	↑	↑	↑		↑	↑
2. Web-based attacks	↑	↑	↑	↑	→		↑	
3. Web application attacks /Injection attacks	↑	↑	↑	↑	↑		↑	↑
4. Botnets	↓		↑	↑				
5. Denial of service	↑	↑		→	→		↑	↑
6. Spam	↓	↑						
7. Phishing	↑		↑		↑	↑	↑	↑
8. Exploit kits	↓		↑		↑		↑	
9. Data breaches	↑			↑		↑		↑
10. Physical damage/theft /loss	↑	↑	↑		↑	↑	↑	↑
11. Insider threat	→	↑		↑		↑	↑	↑
12. Information leakage	↑	↑	↑	↑	↑	↑	↑	↑
13. Identity theft/fraud	↑	↑	↑	↑	↑	↑	↑	↑
14. Cyber espionage	↑	↑		↑	↑	↑		↑
15. Ransomware/ Rogueware/ Scareware	↓		↑					

Legend: Trends: ↓ Declining, → Stable, ↑ Increasing

ENISA Threat Landscape 2014: Überblick über die 15 wichtigsten bewerteten aktuellen Cyber-Bedrohungen und die neuen Trends der ENISA Bedrohungslandschaft. Wie die Abbildung zeigt, steigt das Risiko für digitale Erpressungen und Ransomware-Attacken im Bereich mobiler Endgeräte. (Bild: ENISA)

(BKA) gesperrt, da die Nutzer laut der sich öffnenden Meldung etwas Illegales getan haben sollen. Wird die scheinbare Strafe nicht bezahlt, soll die dauerhafte Verschlüsselung des Smartphones oder Tablets erfolgen, so die Drohung der Angreifer.

Neu ist dabei nicht das Vorgehen der Angreifer, dies wird seit Jahren im PC-Bereich beobachtet. Wie das BKA und der Digitalverband Bitkom mitteilten, gab es bereits im Jahr 2013 ganze 6.754 Fälle von digitaler Erpressung unter Einsatz von Ransomware, von der weltweit unterschiedliche Versionen im Umlauf sind. Neben der Erpressung von Privatpersonen gibt es auch Varianten von Ransomware, die auf die Infektion von Server-Systemen ausgelegt sind und somit auch eine Gefahr für kleine oder mittelständische Betriebe darstellen können, wie Bitkom betont. Neu in den letzten Monaten sind die zunehmenden Attacken auf mobile Geräte.

Digitale Erpressung erlangt enorme Ausmaße

Wie verbreitet und gefährlich die Attacken über Ransomware bereits sind, zeigt zum Beispiel ein Bericht der Cyber Threat Alliance (CTA). Die Studie mit dem Titel „Lucrative Ransomware Attacks: Analysis of the CryptoWall Version 3 Threat“ fasst die Ergebnisse der Untersuchung zu der Entwicklung und zu den globalen Auswirkungen der aggressiven Ransomware CryptoWall zusammen. Die untersuchten Attacken haben den Internetkriminellen Einnahmen von mehr als 325 Millionen US-Dollar beschert. Die Einnahmen stammen aus Lösegeld, das von den Opfern bezahlt wurde, damit ihre Dateien wieder entschlüsselt werden und sie darauf zugreifen können.

Die Analysen der CTA brachten ebenso zum Vorschein: Es gab 406.887 versuchte Crypto-Infektionen mit 4.046 Malware-Varianten. Entdeckt wurden 839 Command & Control-Internetadressen für Server, die von Cyber-Kriminellen verwendet werden, um Befehle zu senden und zu empfangen. Betroffen von den Attacken waren Hunderttausende von Opfern auf der ganzen Welt. Dabei war Nordamerika Ziel der meisten Kampagnen. Doch auch Deutschland gehört zu den bevorzugten Angriffszielen digitaler Erpresser.

Damit sich Unternehmen besser vor Ransomware-Attacken schützen können und eine präventive IT-Sicherheit gegen Online-Erpressungsversuche etablieren, werden in den folgenden Kapiteln dieses eBooks die entsprechenden Schutzmaßnahmen näher vorgestellt. Es ist höchste Zeit, sich gegen die Online-Erpresser zu rüsten. *Oliver Schonschek*

Ransomware: Mehr als eine weitere Malware-Attacke

Angriffe mit Ransomware haben Erfolg, obwohl viele Unternehmen glauben, gegen Malware umfassend geschützt zu sein. Offensichtlich gibt es Sicherheitslücken, an die zu wenig gedacht wird.

Selbst der Basisschutz ist lückenhaft

Umfragen zur IT-Sicherheitsausstattung von Unternehmen wie die Studie „Spionage, Sabotage und Datendiebstahl – Wirtschaftsschutz im digitalen Zeitalter“ vom Bitkom-Verband zeigen regelmäßig, dass es Schwachstellen in der IT-Sicherheit gibt, die Attacken vereinfachen oder sogar zulassen. Wenn es um den Malware-Schutz geht, scheint es jedoch gut auszusehen: Alle befragten Unternehmen setzen Virenscanner, Firewalls sowie einen Passwortschutz für Computer und andere Kommunikationsgeräte ein.

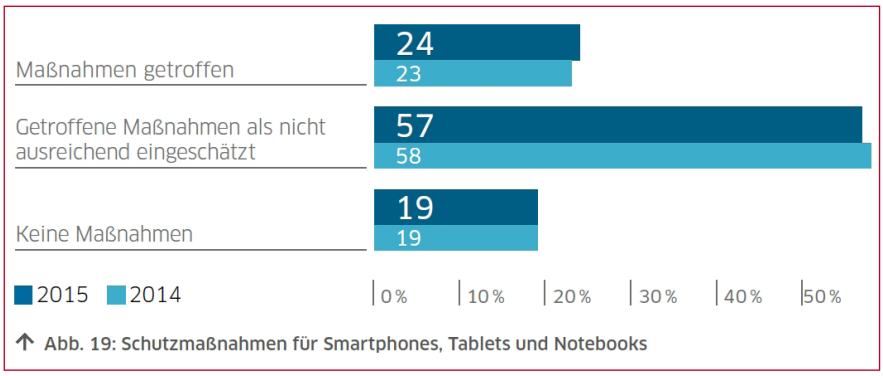


Abb. 19: Schutzmaßnahmen für Smartphones, Tablets und Notebooks

Mobile Endgeräte sind eine erhebliche Schwachstelle in der Unternehmens-IT, das sehen auch die Betroffenen selbst so. (Bild: DsiN-Sicherheitsmonitor 2015)

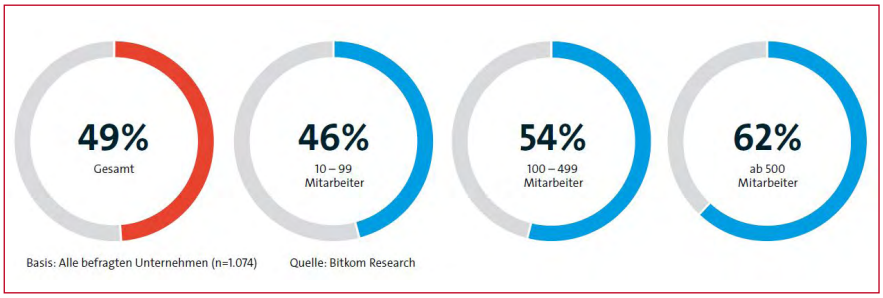
Bei einem umfassenden Anti-Malware-Schutz sollten Schadprogramme wie Ransomware kaum Chancen auf Erfolg haben. Die Berichte über digitale Erpressungsversuche reißen jedoch nicht ab. Im Gegenteil häufen sich die Warnungen zum Beispiel von der US-Bundespolizei FBI vor immer neuen Verschlüsselungsattacken. Offensichtlich reicht der bestehende Malware-Schutz nicht aus.

Mobile Endgeräte werden zum Einfallstor

Im Bereich der mobilen Endgeräte erwartet die EU-Agentur für Netz- und Informationssicherheit ENISA eine steigende Bedrohung durch Ransomware, aus gutem Grund. Smartphones und Tablets sind immer noch nicht so gut gegen Schadsoftware geschützt, wie dies meist bei PCs und Notebooks der Fall ist. So ergab der DsiN-Sicherheitsmonitor Mittelstand 2015 von Deutschland-sicher-im-Netz e.V., dass nur 24 Prozent der befragten kleinen und mittelständischen Unternehmen in Deutschland Maßnahmen zum Schutz mobiler Endgeräte getroffen haben, 57 Prozent schätzen ihre eigenen Maßnahmen als nicht ausreichend ein und 19 Prozent haben nach eigener Aussage gar keine Schutzmaßnahmen für mobile Geräte ergriffen.

Unzureichende IT-Sicherheit auf Tablets und Smartphones erhöht die Chancen für digitale Erpresser gleich mehrfach: Zum

einen können die Daten auf den mobilen Endgeräten gegen den Willen des Nutzers verschlüsselt werden. Selbst wenn die mobilen Daten verschlüsselt vorliegen sollten, was leider oftmals nicht der Fall ist, können Angreifer die Daten zusätzlich verschlüsseln und für den Nutzer unerreichbar machen. Bereits die Verschlüsselung der lokalen Daten auf den mobilen Endgeräten kann großen Schaden mit sich bringen, wenn man an die inzwischen enormen Speicherkapazitäten der Endgeräte in Form von internem Speicher und Speicherkarten denkt.



Laut einer Bitkom-Studie hat nur die Hälfte der Unternehmen ein Notfallmanagement. (Bild: Bitkom)

Aber Ransomware kann noch mehr anrichten, wenn mobile Endgeräte unzureichend geschützt sind: Smartphones und Tablets werden für den Zugriff auf das Firmennetzwerk und auf Cloud-Ressourcen sowie -Anwendungen genutzt. Über den mobilen Zugang könnte es den digitalen Erpressern also gelingen, auch Datenbestände innerhalb des Firmennetzwerkes oder in der Cloud zu verschlüsseln. Dadurch steigt das Schadensrisiko dramatisch an.

Auch das Notfall- und Backupkonzept muss stimmen

Neben unvollständigem Anti-Malware-Schutz gibt es eine weitere, deutliche Schwachstelle im IT-Sicherheitskonzept vieler deutscher Unternehmen: Nur knapp die Hälfte (49 Prozent) aller Unternehmen in Deutschland verfügt über ein Notfallmanagement bei digitaler Wirtschaftsspionage, Sabotage oder Datendiebstahl, so die Umfrage des Digitalverbands Bitkom. Der 5. DsiN-Sicherheitsmonitor Mittelstand zeichnet ein ähnlich düsteres Bild: Ein Viertel der befragten Unternehmen hat kein Datensicherungskonzept. Der Notfallplan ist sogar nur bei knapp einem Drittel der kleinen und mittelständischen Unternehmen vorhanden.

Damit digitale Erpresser kaum noch Chancen haben, müssen Unternehmen in Deutschland also noch einiges für ihren Basisschutz in der IT-Sicherheit tun, von fortschrittlichen Schutzmaßnahmen einmal ganz abgesehen. Umfassender Virenschutz und ein Datensicherungs- und Notfallkonzept müssen umgehend nachgeholt werden, damit nicht mehr Daten verschlüsselt werden, als es dem Unternehmen lieb ist. *Oliver Schonschek*

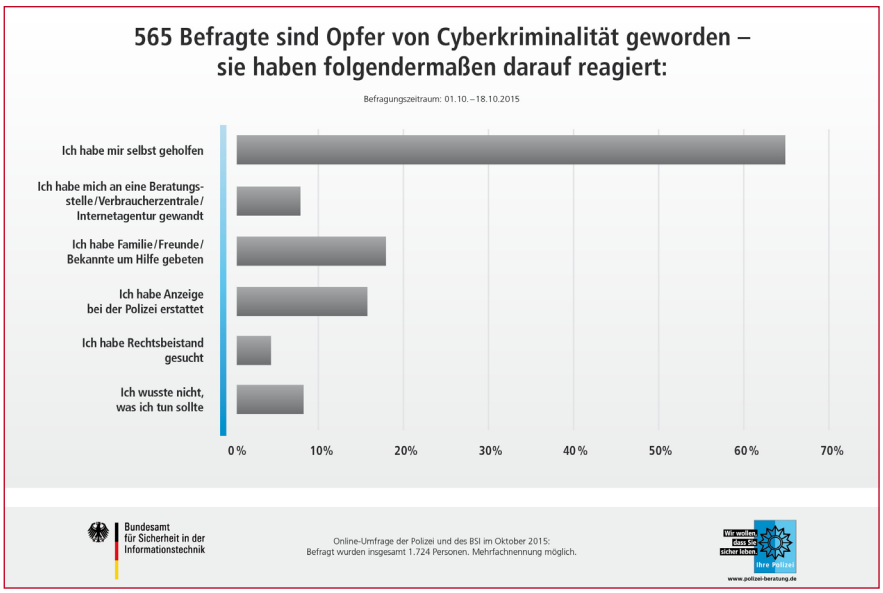
Vollständige Backups als „Plan B“ bei digitaler Erpressung

- Alle Datenquellen in das Backup einbeziehen (auch mobile Systeme und Cloud-Systeme)
- Festlegung der Frequenz und Methode für Backups
- Sichere Aufbewahrung der Backups
- Absicherung der (Online-)Zugänge zu den Backups (starke Zugangskontrolle, Berechtigungssystem)
- Notfallkonzept mit Regelungen zur Datensicherung
- Nutzerschulung über Backups
- Datenübertragung zum Backup verschlüsseln
- Backups automatisieren
- Protokollierung der Backups
- Meldung von Backup-Problemen an die Administration
- Restart-Fähigkeit des Backup-Dienstes

Nicht auf die digitale Erpressung warten

Präventiver Schutz gegen Online-Erpressung

Unternehmen sollten nicht auf die nächste Ransomware-Attacke warten, sondern die Bedrohung ernst nehmen und umgehend handeln. Dazu gehört insbesondere auch die Sensibilisierung der Mitarbeiterinnen und Mitarbeiter.



Umfrageergebnis von Polizei und BSI: „Wie reagieren Opfer auf Cyberkriminalität?“ In der Studie wurde zudem festgestellt, dass selbst das Erleben von Cybercrime bei vielen Betroffenen nicht automatisch dazu führt, sich in Zukunft besser zu schützen. (Bild: BSI / ProPK)

Aus Fehlern lernen

Trotz erhöhter Sensibilisierung wird der Erfolg von Cyber-Angriffen dadurch begünstigt, dass angemessene Sicherheitsmaßnahmen von vielen Anwendern nicht konsequent umgesetzt werden. Man kann von einer digitalen Sorglosigkeit sprechen – sowohl bei Privatanwendern als auch bei Unternehmen, so das Bundesamt für die Sicherheit in der Informationstechnik (BSI). Das bleibt nicht ohne Folgen.

Wie die Cyber-Sicherheits-Umfrage 2015 des BSI zeigt, waren 58 Prozent der Unternehmen und Behörden in den vergangenen zwei Jahren Ziel von Cyber-Angriffen. In 42 Prozent der Fälle waren die Angreifer erfolgreich. Im Vergleich zum Vorjahr stieg die Rate um 8 Prozentpunkte. Den betroffenen Unternehmen entstanden Schäden durch Betriebs- bzw. Produktionsausfälle und Kosten für die Wiederherstellung der betroffenen Systeme.

Eine häufige Ursache für IT-Sicherheitsvorfälle waren unbeabsichtigte Fehlhandlungen durch Mitarbeiter (54 Prozent). Auch dies unterstreicht, dass die digitale Sorglosigkeit ein hohes Risiko darstellt. Das gilt insbesondere auch für den Fall einer digitalen Erpressung: Hier kann aus der Sorglosigkeit schnell Angst und ungeplantes Handeln erwachsen.

Awareness muss deutlich steigen

Selbst nach einer erfolgreichen Attacke steigt das IT-Sicherheitsniveau in betroffenen Unternehmen nicht wie erwartet an, es werden also nicht automatisch weitere IT-Sicherheitsmaßnahmen ergriffen. Eigene Erfahrungen mit Cyber-Kriminalität sind nur für rund die Hälfte der Betroffenen ein Grund, weitere Schutzmaßnahmen zu ergreifen, so ein Ergebnis aus einer Online-Umfrage der Polizei und des BSI.

Unternehmen sind deshalb gefordert, zum einen für einen umfassenden Anti-Malware-Schutz sowie ein Datensicherungs- und Notfallkonzept zu sorgen – gerade auch für mobile Endgeräte. Sie sind aber auch gefordert, die Nutzerinnen und Nutzer im Unternehmen besser zu schulen, damit sie die Risiken durch Online-Erpressung

Nicht auf die digitale Erpressung warten

besser verstehen und an dem präventiven Schutz gegen Ransomware aktiv mitwirken können.

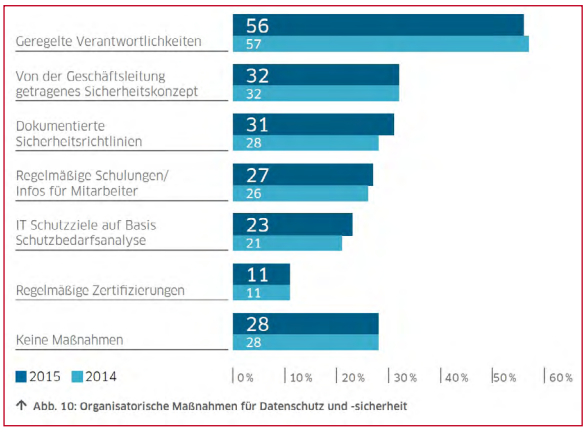


Abb. 10: Organisatorische Maßnahmen für Datenschutz und -sicherheit

Prävention ist sowohl technisch als auch organisatorisch notwendig. Organisatorische Maßnahmen werden häufig vernachlässigt. (Bild: DsiN-Sicherheitsmonitor 2015)

Der Nutzer darf sich nicht erpressen lassen

Bei allen IT-Sicherheitsmaßnahmen, die ergriffen werden müssen, um sich vor digitalen Erpressern zu schützen, kommt der Sensibilisierung ein besonderer Stellenwert zu. Missversteht der betroffene Nutzer die Lage, glaubt er zum Beispiel, die Daten seien ohne Zahlung des Lösegeldes verloren, kann er aus Furcht und in Panik durchaus dazu verleitet werden, das Lösegeld zu bezahlen. Das kann insbesondere dann sein, wenn zusätzlich mit der Veröffentlichung der Daten gedroht wird und der Nutzer zum Beispiel um seinen Arbeitsplatz besorgt ist.

Nur wenn der Nutzer weiß, dass die Daten nicht unbefugt veröffentlicht werden können, da sie bereits verschlüsselt waren, und dass die Daten aus der Datensicherung wiederhergestellt werden können, ist eine besonnene Reaktion zu erwarten. Damit der Betroffene auch die IT-Administration oder die eigene vorgesetzte Stelle von der Ransomware-Attacke informiert, muss allen Beschäftigten klar sein, dass sie nicht dafür bestraft werden, wenn es zu einer digitalen Erpressung gekommen ist. Die psychologischen Mittel der digitalen Erpresser wie Angst und Schuldgefühl bei den Opfern müssen also ebenso abgewehrt werden wie die technischen Angriffswerkzeuge. Prävention ist sowohl technisch als auch organisatorisch Trumpf.

Oliver Schonschek

Präventive Maßnahmen gegen das steigende Risiko durch Ransomware

- Jedes Endgerät muss über eine aktuelle und professionelle IT-Sicherheitslösung abgesichert werden, darunter auch mobile Endgeräte wie Smartphones und Tablets.
- Jedes Endgerät und Betriebssystem sowie jede Anwendung muss aktuell gehalten werden, Fehlerbehebungen (Patches) müssen zeitnah eingespielt werden.
- Sofern das Endgerät oder Betriebssystem dies ermöglicht, sollte die Internetnutzung über ein zweites Benutzerkonto durchgeführt werden, das über keine administrativen Rechte verfügt.
- Für die Internetnutzung sollte nur ein aktueller Browser eingesetzt werden – mit aktuellen Erweiterungen, soweit diese für die betriebliche Nutzung tatsächlich erforderlich sind.
- Jedes Endgerät und jedes Speichermedium, auch die mobilen, müssen bei der regelmäßigen Datensicherung berücksichtigt werden.
- Die Backups dürfen nicht ungeschützt über das Internet erreichbar sein.
- Die Nutzer müssen unterwiesen werden, wie sie auf einen digitalen Erpressungsversuch reagieren sollen: Vollständige Backups sorgen dafür, dass es zu keinem Datenverlust kommt, wenn Ransomware mit ungewollter Verschlüsselung Erfolg hat. Die betroffenen Nutzer sollten auf keinen Fall das Lösegeld bezahlen. Dies ist die eindeutige Empfehlung des Bundeskriminalamtes (BKA). Stattdessen soll die interne IT-Administration eingeschaltet werden, die Geschäftsleitung soll zudem die Polizei einschalten, um den Erpressungsversuch zu melden.
- Die eigene Verschlüsselung vertraulicher Daten sorgt dafür, dass die digitalen Erpresser ihre Drohung, bei Nichtzahlung des Lösegelds die Daten öffentlich zu machen, nicht wahrmachen können. In Kombination mit einem vollständigen Backup verliert so die Ransomware-Attacke viel von ihrem Schrecken.

McAfee Threat Intelligence Exchange und McAfee Advanced Threat Defense

Sicherheit durch Einheit

Anpassbare Sicherheitsdaten ermöglichen die sofortige Reaktion auf neue Bedrohungen.

Zur effektiven Abwehr neuer Bedrohungen benötigen Unternehmen ein Sicherheitssystem, das eine Kombination aus Verhaltens-, Reputations- sowie signaturbasierten Analysen für Netzwerk und Endgeräte bietet. Doch selbst wenn die einzelnen Technologie-Ebenen jeweils gute Leistungen bei der Bedrohungserkennung bereitstellen, ist es wichtig, dass sie eng verzahnt arbeiten, um Daten auszutauschen, Informationen zu erlangen und sich gemeinsam an neue Bedrohungen anzupassen.

McAfee Threat Intelligence Exchange und McAfee Advanced Threat Defense arbeiten verzahnt zusammen, um gemeinsam automatisierten und adaptiven Schutz vor neuen Bedrohungen bereitzustellen. Unabhängig davon, wo der Erstkontakt durch eine unbekannte Malware-Datei stattfand, wird die gesamte vernetzte Umgebung unmittelbar nach der Erkennung aktualisiert. Wenn also eine Datei von McAfee Advanced Threat Defense überführt wurde, veröffentlicht McAfee Threat Intelligence Exchange diese Bedrohungsinformationen in einem Reputations-Update über den McAfee Data Exchange Layer an alle Gegenmaßnahmen im Unternehmen. Endgeräte mit McAfee Threat Intelligence Exchange besitzen somit einen präventiven Schutz, wenn die Datei später erneut gefunden wird. Gateways mit McAfee Threat Intelligence Exchange verhindern, dass die Datei ins Unternehmen gelangt. Und wenn Endgeräte mit McAfee Threat Intelligence Exchange Dateien mit unbekannter Reputation erkennen, werden diese an McAfee Advanced Threat Defense weitergeleitet. Die Lösung überprüft dann, ob das Objekt böswillig ist, und schließt dadurch Erkennungslücken durch die Out-of-Band-Übertragung von Schaddaten.

Wichtige Vorteile

- Erhebliche Verkürzung der Zeitspanne bis zur Eindämmung durch automatisierte und adaptive Bedrohungsreaktion
- Bessere Übersicht, Flexibilität und Kontrolle durch Vernetzung des Netzwerk- und Endgeräteschutzes
- Intelligente Reaktion auf Zwischenfälle dank zuverlässiger Datei-Reputation und Informationen zur Ausführung
- Verbesserte Sicherheit bei optimierten Gesamtbetriebskosten durch vereinfachte Integration und Implementierung

Schließen der Sicherheitslücke

Erkennung verborgener Malware-Schaddaten

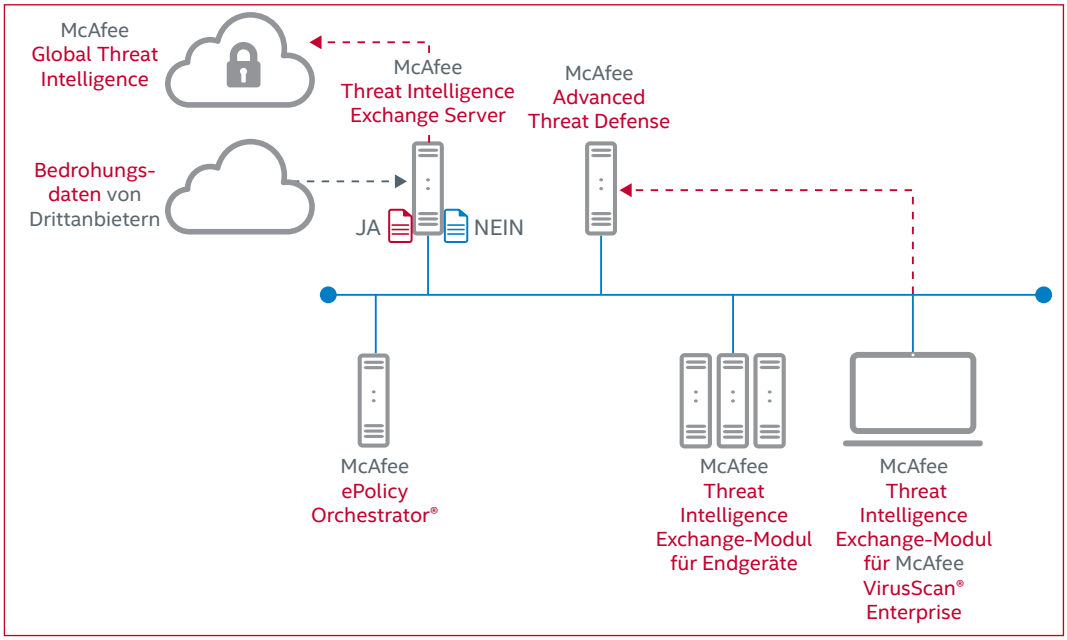
McAfee Threat Intelligence Exchange und McAfee Advanced Threat Defense agieren gemeinsam, um verdächtige Objekte unabhängig vom Erstkontakt zu analysieren. Sobald der Versuch gestartet wird, neue Dateien auszuführen, werden sie in dieser kooperativen Lösung den gemeinsamen Endgeräteregeln, Umgebungs- und weltweiten Reputationsinformationen sowie tiefgehenden statischen und dynamischen Analysen der verbundenen Komponenten unterzogen. Dieser vernetzte Ansatz zur Bedrohungsanalyse ermöglicht eine genauere Erkennung verborgener Malware, die andernfalls unentdeckt bleiben würde.

Verbesserung der Bedrohungserkennung durch verhaltensbasierte Bedrohungsanalyse

McAfee Advanced Threat Defense ermöglicht die Reputationsklassifizierung durch

McAfee Threat Intelligence Exchange und McAfee Advanced Threat Defense

innovative Möglichkeiten zur Malware-Dekonstruktion, zu denen unter anderem leistungsstarke Entpackungsfunktionen gehören. Diese können Verschleierungstechniken aushebeln und den ursprünglichen ausführbaren Code offenlegen, was die Erkennung des beabsichtigten Verhaltens ermöglicht. Gemeinsam ermöglichen dynamische und statische Code-Analysen eine vollständige Bewertung und bieten eine der leistungsfähigsten Technologien zur Erkennung hochentwickelter Bedrohungen auf dem Markt.



Daten- und Reputations-Synthese aus der Cloud, dem Netzwerk sowie von Endgeräten (Bild: Intel Security)

Einbindung von Security Connected durch den McAfee Data Exchange Layer

McAfee Threat Intelligence Exchange nutzt den McAfee Data Exchange Layer. Diese extrem schnelle und Ressourcen-schonende bidirektionale Kommunikationsstruktur erlaubt die Integration von Produkten sowie den Austausch von Kontextinformationen. Auf diese Weise kann sie Sicherheitsinformationen und adaptiven Schutz bereitstellen. Produkte, die den McAfee Data Exchange Layer nutzen, melden sich einfach an der Struktur an und können ihrerseits Daten veröffentlichen. Dabei ist keine komplexe API-basierte Integration oder aufwändige Konfiguration notwendig. Der Beginn einer neuen Sicherheitsära, in der alle Komponenten gemeinsam als zusammenhängendes System arbeiten.

Übersicht und Kontrolle vom Endgerät bis zum Netzwerk

McAfee Advanced Threat Defense erfasst Malware-Exemplare, die von anderen Produkten in der Unternehmensumgebung an Netzwerkeintrittspunkten gesammelt wurden. Die Netzwerkkomponenten können wiederum die neuen Erkenntnisse aus diesen Exemplaren über McAfee Threat Intelligence Exchange teilen. Dieser Daten- und Reputationsaustausch verdeutlicht die Vorteile des Informationsaustauschs zwischen Endgeräten und Netzwerkkomponenten im Rahmen der McAfee Security Connected-Plattform von Intel Security. Zudem verwaltet McAfee Threat Intelligence Exchange eine KnowledgeBase mit Informationen darüber, wo die letzten Objekte in der Endgeräteumgebung ausgeführt wurden, um so eine umfassende Übersicht aller Zwischenfälle bereitzustellen.

Adaptive Reaktionen

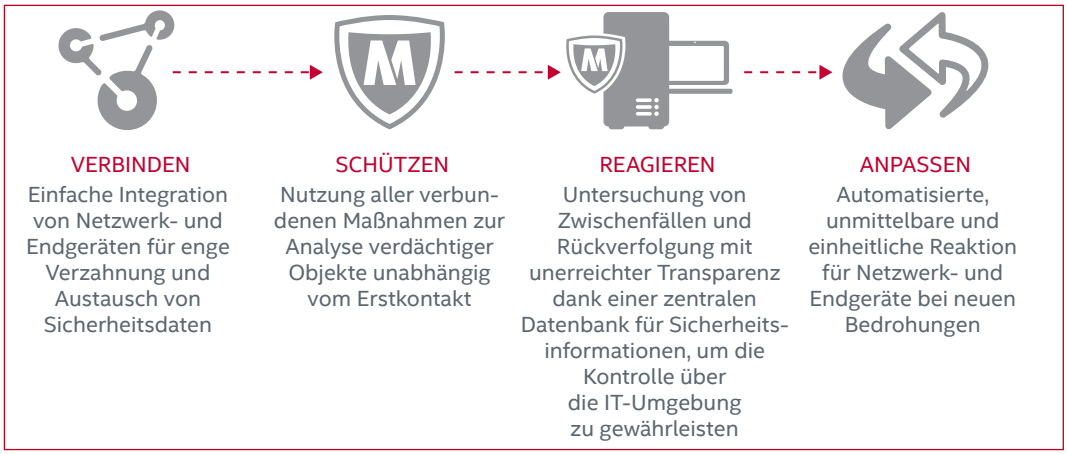
Sobald McAfee Advanced Threat Defense eine Datei analysiert und klassifiziert hat, werden die Ergebnisse an McAfee Threat Intelligence Exchange gesendet. Die neue Datei-Reputation (ganz gleich, ob sie gut oder schlecht ist) wird sofort für alle Gegenmaßnahmen mit McAfee Threat Intelligence Exchange in der gesamten Umgebung veröffentlicht. Von da an wird jedes weitere Exemplar der Datei erkannt, sodass sie von allen Komponenten mit McAfee Threat Intelligence Exchange entsprechend ihren Richtlinien zugelassen, blockiert oder bereinigt wird. Diese adaptiven Reaktionen bieten sofortigen Schutz für die gesamte Umgebung, einschließlich des Netzwerks, des Gateways und der

McAfee Threat Intelligence Exchange und McAfee Advanced Threat Defense

Endgerätekomponenten. Die Reaktionsgeschwindigkeit wird beschleunigt und die Zeitspanne bis zur Eindämmung sowie Behebung erheblich verkürzt – und das alles ohne Netzwerkumbau.

Einfache Bereitstellung und Verwaltung

Die Verzahnung zwischen McAfee Threat Intelligence Exchange und McAfee Advanced Threat Defense erfolgt nahtlos über den McAfee Data Exchange Layer. Dieser wurde als offenes Framework konzipiert und erlaubt Sicherheitskomponenten die dynamische Einbindung in McAfee Threat Intelligence Exchange, ohne dass umfangreiche APIs oder komplexe Produktkonfigurationen erforderlich sind. Dies ermöglicht die Senkung der Fehlerhäufigkeit und vermeidet einen umfangreichen manuellen Aufwand.



Dank dem Security Connected-Ansatz erhalten Unternehmen über den Data Exchange Layer eine nahtlose Integration (Bild: Intel Security)

Fazit

McAfee Threat Intelligence Exchange und McAfee Advanced Threat Defense sind unverzichtbare Lösungen, die separate Sicherheitskomponenten verbinden, die gesamte Unternehmensumgebung schützen, auf Zwischenfälle reagieren und sich automatisch an neue Bedrohungen anpassen. Mit einem Sicherheits-Ökosystem, das modernste Bedrohungsanalyse, Netzwerkprodukte und Endgerätelösungen miteinander vernetzt, ermöglicht Intel Security unternehmensweite Transparenz und Kontext für Bedrohungen bei gleichzeitiger Verkürzung der Reaktionszeit und Vereinfachung der Problembehebung.