Einzelheftpreis € 15,-

4/2016 Februar April Juni **September** Oktober Dezember

IT-SICHERHEIT

Fachmagazin für Informationssicherheit und Compliance

Zielgenaue Strategien als Schutz vor aktuellen Angriffen

Interview Mario Emig, Head of Information Security, Business Development bei Controlware

Storage

- Flash-Storage: Basis für höhere Datenverfügbarkeit
- Software Defined Storage (SDS): Optimal mit Flash
- Backup-Tipps für Big Data

Szene

- Tagung: „Vertrauen und Vergessen (werden) in der digitalen Gesellschaft“
- Datenträgervernichtung: Am Bedarf vorbei standardisiert! (Gastkommentar)

Trends und Technik

- Im Test: Altaro VM Backup 6.2.2.0
- Roboter: Sicher und vertrauenswürdig?
- Big Data: Chance für den Mittelstand?

DATAKONTEXT www.itsicherheit-online.com

Interview mit Mario Emig, Head of Information Security, Business Development bei Controlware

„Zielgenaue Strategien als Schutz vor aktuellen Angriffen!“

Als einer der führenden unabhängigen deutschen Systemintegratoren und Managed Service Provider unterstützt Controlware seit Gründung im Jahr 1980 seine Kunden mit Komplettlösungen und Dienstleistungen in der Informationstechnologie. Dabei verfolgt das Unternehmen den Grundsatz, die spezifischen Problemstellungen seiner Kunden immer in den Mittelpunkt der Projekte zu stellen. Im Interview mit IT-SICHERHEIT verrät Mario Emig, Head of Information Security und Business Development bei der Controlware GmbH, was Unternehmen im Angesicht aktueller Bedrohungen wie Ramsomware (Verschlüsselungstrojaner) und DDoS-Attacken tun sollten, um sich bestmöglich dagegen zu schützen.

ITS: Herr Emig, was waren in diesem Jahr bisher die Top-Themen für den Bereich Informationssicherheit? Mit einer Prognose sollten Sie ja schon mal Recht behalten: Sie hatten bereits sehr früh vor Verschlüsselungstrojanern gewarnt.
Mario Emig: In der Tat hatten wir bereits bei unserer Controlware Security Roadshow, die wir traditionell zu Beginn des Jahres in mehreren Städten in Deutschland durchführen, vor Verschlüsselungstrojanern als eine der Security-Herausforderungen in 2016 gewarnt. Zu dem Zeitpunkt, als wir die Security-Trends für das kommende Jahr prognostiziert haben, war Locky noch nicht aktiv. Allerdings gab es neben FBI-Berichten über dramatische prozentuale Steigerungsraten auch in den bekannten Foren entsprechende Hinweise.

Die Tatsache, dass mit dieser Art von Cyber-Erpressung sehr viel Geld zu verdienen ist, verstärkte dann die Angriffe zusätzlich. Vielleicht weckte sogar die prominente Berichterstattung zu diesem Thema zusätzlich Begehrlichkeiten bei Kriminellen.

ITS: Auch bei Distributed Denial of Service (DDoS)-Angriffen werden wie bei Verschlüsselungstrojanern oft Gelder erpresst. Sehen Sie hier Parallelen?
Mario Emig: Das ist ein guter Vergleich. In beiden Fällen gibt es professionelle, kriminelle Organisationen, die es sich zum Ziel gemacht haben, die IT-Infrastrukturen von Unternehmen zu stören und quasi gegen den Einwurf von Münzen wieder „freizugeben“. DDoS-Angriffe konzentrieren sich allerdings mehr auf Unternehmen. Hier geht es neben dem Versuch, Gelder zu erpressen auch darum, Konkurrenten zu schaden. Angreifer suchen sich ihre Ziele ganz bewusst aus und attackieren diese dann gezielt. Ist ein Unternehmen sehr stark auf seine Internetpräsenz angewiesen – beispielsweise ein Online-Shop oder eine Bank mit Online-Banking – ist auch ein kurzer Systemausfall nicht hinzunehmen und kostet die betroffenen Unternehmen, neben einem nicht so einfach monetär zu beziffernden Reputationsschaden, direkt Geld.

Bei Verschlüsselungstrojanern hingegen ist das Ziel eher die anonyme Masse. Gerade Privatpersonen, die plötzlich nicht mehr auf ihre Familien- und Urlaubsbilder zugreifen können, sind schnell bereit, mal eben 20, 50 und mehr Euro zu zahlen, um ihre Daten zurückzubekommen.

ITS: Bleiben wir noch kurz bei den DDoS-Angriffen. Wie häufig kommen diese Angriffe vor, wer sind die Angreifer und wie können sich Kunden schützen?
Mario Emig: Laut CERT-Bund sind Angriffe auf Webseiten beispielsweise bei der Bundesverwaltung aktuell die zweithäufigste Angriffsform. Auch andere Behördenseiten sind häufig betroffen. Bei Behörden sind Angriffe für gewöhnlich politisch motiviert, bei Un-

ternehmen geht es wie bereits geschildert fast ausschließlich um konkrete Geldforderungen. Zunächst müssen Kunden eine Risikoabschätzung treffen. Was passiert, wenn man betroffen ist? Was kostet ein Ausfall? Wie wahrscheinlich ist ein Angriff? Hierbei ist es wichtig zu wissen, dass bei entsprechenden Angriffen nicht nur Webseiten wie Online-Shops ausfallen können, sondern beispielsweise auch ERP- und andere Systeme in Mitleidenschaft gezogen werden – was auch schnell zum Ausfall der Kommunikation mit Kunden führen kann.

> „Man sollte sich auch nicht ausschließlich auf eine weitere technische Maßnahme wie etwa Sandboxing verlassen, sondern an dieser Stelle die Gelegenheit nutzen, die gängigen internen Security-Prozesse auf den Prüfstand zu stellen."

Vor der Einführung einer technischen Lösung sollten auf jeden Fall entsprechende Notfallpläne vorhanden sein. Hierbei kann es sich durchaus um Festlegungen handeln, wer bei einer Störung zu kontaktieren ist oder wer im Unternehmen wann welche Entscheidungen trifft. Solche Notfallpläne können auch die Kontaktdaten der Ansprechpartner bei einem Provider einschließen.

Technisch gesehen gibt es grundsätzlich zwei Lösungen: On-Premise oder Cloud-basiert. Volumenattacken lassen sich über einen Cloud-basierten DDoS-Schutz in der Regel recht zuverlässig abfangen. Hierbei wird der Traffic entweder immer oder eben nur im Angriffsfall auf ein solches Cloud-basiertes Data Center umgeleitet. Applikations-basierte Attacken hingegen lassen sich am besten mit On-Premise-Systemen stoppen. Das liegt daran, dass für einen Angriff häufig verschlüsselte HTTPS-Verbindungen genutzt werden und der Kunde die hierfür benötigen Schlüssel im Regelfall nicht außer Haus geben möchte.

ITS: Welche Erfahrungen haben Sie bisher mit den unterschiedlichen Systemen gemacht?
Mario Emig: Die meisten unserer Kunden, die sich gegen DDoS-Angriffe absichern, nutzen eine Kombination aus den beiden beschriebenen Methoden. Zunächst filtert man mit entsprechender Hardware-Appliance, also einem Anti-DDoS-System, selbst den Verkehr. Hier besonders mit Blick auf bereits erwähnte Applikationsbasierte Attacken. Besteht die Gefahr, dass die Pipe vollläuft, wird rechtzeitig auf ein Cloud-basiertes System umgeschaltet. Dieser Vorgang wird nach im Vorfeld festgelegten Schwellenwerten automatisch durchgeführt. Meistens liegen bereits weiterführende Erkenntnisse über die Methoden der Angreifer vor. Diese Erfahrungen sind bei einer Attacke äußerst hilfreich. Wichtig ist, schnell die richtigen Entscheidungen zu treffen.

ITS: Was hat sich im Vergleich zu früheren Angriffen beziehungsweise Infektionen mit Viren geändert?
Mario Emig: Es sind ganz klar die professionellen Strukturen, mit denen Angreifer agieren. Die Zeiten, als Webseiten gehackt wurden, um den Namen der Hackergruppe dort zu hinterlassen, sind nahezu vorbei. Angreifer haben heute in der Regel klare monetär geprägte Ziele.

ITS: Brauchen Angreifer heute mehr Spezialwissen für Angriffe als früher? Ich erinnere mich noch daran, als zum ersten Mal Virenbaukästen zum Download für jedermann im Internet auftauchten.
Mario Emig: Diese Frage möchte ich nicht pauschal mit ja oder nein beantworten. Es gab in der Tat in der Vergangenheit diverse Virenbaukästen, die zum Teil mit grafischen Oberflächen ausgestattet waren. Mit wenigen Klicks konnten sich damit einfache „Viren" erstellen lassen. Diese wurden allerdings auch von Antiviren-Software recht zuverlässig erkannt.

Ähnliche Systeme gibt es auch für DDoS-Angriffe. Zum einen ist es damit möglich, Trojaner zu erstellen, die sich dann später als Bot-Netz für einen DDoS-Angriff verwenden lassen. Zum anderen sieht das Geschäftsmodell von Kriminellen so aus, dass Angriffe als Dienstleistung eingekauft werden können.

ITS: Und die Verschlüsselungstrojaner?
Mario Emig: Selbst bei den Verschlüsselungstrojanern gibt es bereits Baukastensysteme. Derjenige, der einen Betrag x erpressen möchte, gibt eine Bitcoin-Adresse und die Höhe des zu erpressenden Betrags an. Eine Webseite generiert dann den Trojaner. Der Erpresser ist für die Verteilung verantwortlich und muss noch eine Beteiligung (etwa 20 Prozent der erpressten Summe) abgeben. So werden also auch für die Programmierer beziehungsweise Hintermänner des Baukastensystems komfortabel Einnahmen generiert. Der Angreifer benötigt kein Spezialwissen. Es gibt aber auch weitere Facetten hinsichtlich der Geschäftsmodelle.

ITS: Warum waren die Verschlüsselungstrojaner wie Locky so erfolgreich und warum gelingt es der gängigen Antiviren-Software nicht, diese zu stoppen?

Die Locky-Entwickler haben das Tool ständig weiterentwickelt und neue Mechanismen implementiert, um Antiviren-Programme zu überlisten. Neue Varianten wurden häufig erst zwölf Stunden, nachdem eine neue Variante im Umlauf war, zuverlässig erkannt. Genug Zeit, um Tausende neue Opfer zu finden

ITS: Die ständig neuen Varianten von Schadcode, man spricht von mehr als 50.000 neuen Schädlingen täglich. Ist das nicht ein generelles Problem von Antiviren-Software?
Mario Emig: Das ist in der Tat ein Problem von Signatur-basierten Systemen. Diese können Malware erst dann erkennen, wenn eine entsprechende Signatur vorliegt. Das bringt uns zu einem neuen Trend, den wir auf der Herstellerseite beobachten. Es gibt immer mehr Hersteller, die den Anspruch haben, Schadcode nicht mehr nur Signatur-basiert zu erkennen, sondern Algorithmen beziehungsweise mathematische Methoden nutzen, um proaktiv Advanced Persistent Threats und Malware zu verhindern und nicht nur reaktiv auf-

zuspüren. Das Wissen über Angriffsvektoren wird also mit Verfahren aus dem Bereich der künstlichen Intelligenz für einen wirksamen Schutz genutzt. Diese Systeme gibt es sowohl Netzwerk-basiert als auch Endpoint-basiert.

ITS: „Antivirus ist tot!", behauptete vor etwa zwei Jahren bereits Brian Dye gegenüber dem Wall Street Journal – damals immerhin Senior-Vizepräsident bei Symantec. Ist dem wirklich so?
Mario Emig: Wir dürfen davon ausgehen, dass er damit nicht Antivirus meinte, sondern eben die Signatur-basierte Virenerkennung. Neben den erwähnten neuen Herstellern, die auch die Branche durchaus mit ihren neuen, auf künstlicher Intelligenz beruhenden Systemen weiter aufmischen könnten, waren auch die etablierten Hersteller nicht untätig. Auch sie haben ihre Antivirus-Suiten um verschiedene neuere Techniken und zusätzliche Mechanismen, wie beispielsweise Heuristiken, Sandboxing, Cloud-Analyse, Whitelisting, URL-Blocker, erweitert.

ITS: Welche Entwicklung wird sich am Endpoint durchsetzen und was bringt Sandboxing?
Mario Emig: Ich bin der Meinung, dass Signatur-basierte Systeme in der Tat an ihren Grenzen angekommen sind. Es macht also durchaus Sinn, diese entsprechend um intelligentere Ansätze zu erweitern. Ich gehe auch davon aus, dass die etablierten Hersteller ihre Antivirus-Systeme noch deutlich weiter ausbauen werden. Einige werden das über Eigenentwicklungen tun, andere – wie in der Branche üblich – durch entsprechende Technologiezukäufe.

Sandboxing ist eine Technologie, die bereits weit gereift ist. Anfängliche Schwächen, wie die Erkennbarkeit einer simulierten Umgebung, in der die Malware brav die Füße stillhält, sind mit unterschiedlichen Methoden behoben. Daher schützt sie inzwischen recht zuverlässig vor unbekannten Bedrohungen. Kunden, die bereits mit Sandboxing-Technologien – egal ob Endpoint-basiert oder Netzwerk-basiert – ausgestattet waren, konnten sich vor Locky und weiteren Verschlüsselungstrojanern überwiegend gut schützen.

ITS: Welche Vorgehensweise würden Sie im Allgemeinen zum Schutz vor Verschlüsselungstrojanern empfehlen?
Mario Emig: Hier gibt es leider nicht die eine Empfehlung, die dann zuverlässig vor jeder Ransomware schützt. Man sollte sich auch nicht ausschließlich auf eine weitere technische Maßnahme wie etwa Sandboxing verlassen, sondern an dieser Stelle die Gelegenheit nutzen, die gängigen internen Security-Prozesse auf den Prüfstand zu stellen. Neben den technischen Maßnahmen wie Sandboxing gibt es nämlich eine ganze Reihe von schnell umsetzbaren Maßnahmen – zum Beispiel Makros in Office-Dokumenten zu blockieren oder Dateianhänge in E-Mails zu sperren, zumindest bei akuten Angriffswellen. Darüber hinaus sollte man den Dateiaustausch über Managed-File-Transfer-Lösungen organisieren und IPS-Signaturen für die Landing Pages von Exploit-Kits auf „Prevent" setzen. Bot-Kommunikation wie Tor, I2P etc. gilt es zu blocken, ebenso wie das Ausführen von Code unter den bekannten Pfaden. Weitere wichtige Maßnahmen sind die Sperrung des Zugriffs auf CMD und Powershell für Standard-Benutzer und generell die Vermeidung von Anmeldung und Arbeiten mit Administrator-Rechten. Sehr hilfreich ist es, die Verwaltung beziehungsweise Trennung von Rechten bei Benutzern und Prozessen konsequent durchzuführen, regelmäßige Backups zu fahren und die gesamte Software inklusive Betriebssystem auf dem aktuellen und somit sichersten Stand zu halten. Das gilt natürlich auch für die Antiviren-Software.

Eine einzige Maßnahme allein ist also in der Regel zu kurz gegriffen. Vielmehr geht es sowohl bei Ransomware als auch bei allen anderen intelligenten Angriffsformen immer darum, ein auf die individuelle Situation beim Kunden zugeschnittenes Strategiepaket zu schnüren, das technische und organisatorische Maßnahmen in idealer Weise kombiniert. Und das ist eine Kunst, bei der wir als Systemintegrator unseren Kunden sehr gerne beratend zur Seite stehen.

ITS: Vielen Dank für das Gespräch!

Das Interview führte Stefan Mutschler, stellvertretender Chefredakteur IT-SICHERHEIT