Die Security-Messlatte steigt: Gefährliche Zeiten für Unternehmen

Eine aktuelle ESET-Studie hat die größten Sicherheitsanforderungen aufgedeckt, mit denen sich Großunternehmen aktuell auseinandersetzen müssen. Im Interview definiert Michal Jankech, Principal Product Manager bei ESET, welchen Unsicherheitsfaktoren Unternehmen ausgesetzt sind und wie sie der höheren Messlatte an IT-Security gerecht werden.

Die fünf Mammutaufgaben für große Unternehmen:

1. Ransomware
2. Gezielte Angriffe und Hacking
3. Unterschiedliche Betriebssysteme im hybriden Netzwerk
4. Fehlendes Sicherheitsbewusstsein der Mitarbeiter
5. Arbeitskräftemangel

ESET hat vor Kurzem Sicherheitslösungen für das Enterprise-Segment vorgestellt. Bei der Entwicklung arbeitete ESET eng mit Großunternehmen zusammen, um ihre Erwartungshaltung an Security-Lösungen zu verstehen. Gerade weil die IT-Sicherheit ein richtig heißes Thema ist, stellt sich die Frage, ob diese Unternehmen bereitwillig zugaben, jemals Opfer eines Cyberangriffs geworden zu sein?

Michal Jankech: Durch eine Geheimhaltungsvereinbarung im Vorfeld stellte sich keine Vertrauensfrage. Außerdem verstehen die Entscheider heute, dass es besser ist, die Security-Probleme zu benennen, auch wenn das mit der Preisgabe sensibler Informationen verbunden ist. Denn eben diese Daten können uns als Anbieter ihrer Sicherheitslösungen dabei helfen, in Zukunft ähnliche Angriffe zu verhindern. In einigen Fällen war genau dieser Austausch sogar der Grund, warum sich Unternehmen für einen Wechsel zu ESET entschieden haben. Es gab auch Unternehmen mit veralteten oder schlecht konfigurierten Security-Anwendungen.

Aus unserer Sicht ist der Zugang zu diesen Informationen unerlässlich. Ein qualitativ hochwertiges Produkt allein reicht nicht mehr aus: Umfassende Informationen, Konfiguration und Implementierung sind ebenso entscheidend. Das bedeutet, dass es immer Raum für Verbesserungen gibt, beispielsweise bei Dokumentations-, Support- oder Imple-

mentierungsleistungen. Unser Ziel ist es, dass unsere Kunden das Produkt korrekt installieren und optimal nutzen. Oder dass wir ihnen alternativ die gleiche Funktion als Dienstleistung anbieten können.

Haben Sie während der Interviews mit den Unternehmen etwas erfahren, was sie wirklich überrascht hat?

Michal Jankech: In einigen Fällen war ich tatsächlich sehr überrascht, wie hoch die Toleranz einiger Unternehmen und Organisationen gegenüber Sicherheitsproblemen ist. Für einige Firmen war es sogar noch völlig ausreichend, wenn zehn Prozent ihres Netzwerks Probleme meldeten. Vor allem im Bildungsbereich war ein solches Verhalten häufig zu beobachten. Die Gründe dafür liegen vermutlich in den fehlenden finanziellen und auch personellen Ressourcen.

Im Rahmen der Kundenbefragungen wurden die Unternehmen gebeten, aus ihrer Perspektive heraus die fünf wichtigsten Sicherheitsprobleme zu benennen. Ganz oben auf der Liste steht Ransomware, also Erpresser-Software, die den Inhalt eines Geräts blockiert und Lösegeld verlangt, um den Zugriff auf die Daten wiederherzustellen. Ransomware gibt es schon seit Jahren, warum ist sie für Unternehmen noch immer so problematisch?

Michal Jankech: In der Vergangenheit wurde Ransomware als Bedrohung Nummer eins gehandelt. Kein Wunder, da Angriffe wie WannaCry und NotPetya Milliardenschäden verursachten und so die Top-Medien der Welt eroberten. Selbst eine Person ohne eigene „Ransomware-Erfahrung" wusste sie als ernsthafte Bedrohung einzuordnen. In den Interviews erfuhren wir, dass unsere Kunden in diesem Bereich weitere Handlungsfelder für uns sahen.

Unsere Telemetrie-Ergebnisse zeigen aktuell ein anderes Gefahrenbild. Demnach hat Phishing erst kürzlich Ransomware vom Thron gestoßen und gilt aus unserer Sicht die Top-Gefahr für Unternehmen dar. Tatsächlich funktionieren beide Bedrohungen nach dem gleichen Prinzip. Angreifer versuchen, das geringe Sicherheitsbewusstsein eines Mitarbeiters auszunutzen, um Schadcode ins Netzwerk eines Unternehmens einzuschleusen.

Wie sind Sie dieses Thema intern angegangen?

Michal Jankech: Wir bieten unseren Kunden seit langem eine sehr gute verhaltensbasierte Malware-Erkennung. Wir hatten bereits HIPS (Host-based Intrusion Prevention System), mit dem Kunden benutzerdefinierte Regeln festlegen konnten, die sie vor Ransomware schützen. Frühzeitig haben wir unser „Ransomware Shield" entwickelt, ein spezifisches Verhaltensmodul mit der Fähigkeit, die Verschlüsselungs-Malware anhand ihres Verhaltens und ihrer Aktivität zu erkennen. Dies ist jedoch die allerletzte Instanz, falls die Bedrohung unbemerkt durch alle vorherigen Sicherheitsebenen schlüpft.

Um das zu verhindern, ist es am besten, potenzielle Ransomware zu überprüfen und zu erkennen, bevor sie ins Netzwerk gelangt. Wir haben festgestellt, dass die E-Mail der stärkste Verbreitungskanal bleibt. In der Regel beginnt alles mit dem Anklicken eines verdächtigen Links, z.B. zu einer vermeintlichen Rechnung eines Zustelldiensts. Deshalb haben wir eine Lösung entwickelt, die wie folgt funktioniert: Sie verschiebt die verdächtige E-Mail oder Kommunikation in eine sichere Sandbox-Umgebung. Dort simuliert sie das Verhalten des Benutzers, das heißt, sie öffnet die E-Mail, klickt auf den Link, lädt den Anhang herunter und löst schließlich die Infektion aus. Dank unserer Erkennungsmodule und Machine Learning wird der Kunde anschließend informiert, ob die E-Mail bösartig ist.

Aber was ist die eigentliche Ursache für solche Infektionen? Geschickte Angreifer oder unvorsichtige Mitarbeiter?

Michal Jankech: Was hat die Verbreitung von WannaCry verursacht? Betriebssysteme ohne Sicherheitspatches. Angreifer nutzten eine bekannte Schwachstelle aus, sodass die einzigen präventiven Maßnahmen eines Unternehmens darin bestanden, sich gegen die Infektion „impfen

zu lassen". Das heißt also, die verfügbaren Sicherheitspatches zu installieren. Die Unternehmen, die das nicht taten, litten unter den Folgen.

Gezielte Angriffe und Hacking belegen den zweiten Platz in der Liste. Sind große Unternehmen wirklich echten Bedrohungen ausgesetzt oder ist es eher die Angst vor solchen Angriffen, wie sie die Medien anheizen?

Michal Jankech: Unternehmen haben diese Probleme tatsächlich. Wir sehen vor allem in den westlichen Ländern, dass es bestimmte Arten von Angriffen gibt, die speziell auf die Geschäftsaktivitäten des jeweiligen Unternehmens ausgerichtet sind. Gezielte Angriffe werden zum Beispiel auch im Wettbewerbskampf eingesetzt. Ziel solcher Attacken ist in den meisten Fällen Spionage, also die Beschaffung geheimer und sensibler Unternehmensinformationen.

Die Unternehmen erwähnen auch den Fachkräftemangel im IT-Bereich. Wie bewerten Sie die Situation?

Michal Jankech: Was die IT betrifft, ist die Situation weniger dramatisch. Im Bereich der IT-Sicherheit stehen wir allerdings vor einem größeren Problem. Einen guten IT-Profi zu finden, ist eine echte Herausforderung, aber einen guten IT-Sicherheitsspezialisten zu finden, fast unmöglich. Fehlt es einem Unternehmen an IT-Sicherheitsexperten, sind wir noch nicht komplett im Worst-Case-Szenario angekommen. In vielen kleinen und mittleren Unternehmen wird die IT als notwendiges Übel wahrgenommen - zum Beispiel im Gesundheitswesen. Das führt zu einem enormen Outsourcing-Trend und wachsenden Kundenerwartungen beim Kauf eines bestimmten Produkts. Je größer das Kundenunternehmen, desto spezifischer sind in der Regel dessen Erwartungen. Im Bereich Enterprise erwarten Entscheider maßgeschneiderten Service - spezielle Ansätze, Präsentationen und Anpassungen, wenn etwas nicht ihren Bedürfnissen entspricht. Nahezu jedes Unternehmen in diesem Segment hat individuelle Anforderungen, sodass sich auch die Implementierungskosten unterscheiden. Vor der Implementierungsphase führen wir eine Bedarfsanalyse durch und geben dem Kunden Empfehlungen für Maßnahmen, die für das Unternehmen in Bezug auf seine physische Kapazität, Netzwerktopologie etc. geeignet sind. Aus diesem Grund haben wir mehrere Pakete für die Unternehmenslandschaft geschnürt. Dazu gehören neben den Produkten und Lösungen auch die Dienstleistungen unserer IT-Sicherheitsexperten.

Viele Unternehmen verwenden längst nicht mehr nur Windows-Geräte. Es ist durchaus üblich, dass ein IT-Team die Sicherheit von fünf verschiedenen Betriebssystemen überwacht - Windows, Linux, Mac, Android und iOS. Inwiefern ist gerade der Mac ein Problem?

Michal Jankech: Unsere Daten zeigen, dass die meisten großen Unternehmen - diejenigen mit mehr als 1000 Arbeitsplätzen - mindestens einen Mac-Computer in ihrer Infrastruktur haben. Es gibt zwei Gründe für deren Vorhandensein in Netzwerken. Sie sind seit langem sehr begehrt bei Mitarbeitern in kreativen Berufen - zum Beispiel in internen Grafikteams, der Marketing- oder Werbeabteilung. Hier wird der Mac wegen eines klaren Geschäftsbedürfnisses verwendet. In anderen Fällen ist es vor allem eine Frage der persönlichen Präferenz der Mitarbeiter oder des Managements.
Problematisch ist: Viele Anwender glauben nach wie vor, dass das Mac-Betriebssystem von Natur aus sicherer ist als Windows. Dies ist jedoch eine verzerrte Sichtweise. Sie wird dadurch verursacht, dass sich Angreifer auf Betriebssysteme konzentrieren, die in größerem Umfang eingesetzt werden – wie beispielsweise Windows. Es gibt jedoch viele Beispiele für Mac-Malware und die Tendenz ist beunruhigend: Immer mehr und immer gefährlichere Schädlinge kommen auf den Markt. Anwender sollten sich nicht in einer falschen Sicherheit wiegen.