

AKAMAI-KUNDENREFERENZ

Universität Tunghai

Akamai Secure Internet Access Enterprise verbessert die Sicherheit der Universität Tunghai und reduziert den Zeitaufwand für das Vorfallsmanagement

Universität entlastet dank Akamai das Sicherheitsteam und reduziert externe Sicherheitsbenachrichtigungen

Moderne Unternehmen sind komplexen Cyberbedrohungen ausgesetzt, da Angreifer immer ausgefeiltere Methoden zur Umgehung von Schutzmaßnahmen verwenden. Wie lässt sich der nötige proaktive Schutz vor solchen Angriffen mit der nötigen Flexibilität und Freiheit in einer großen, internationalen Hochschule in Einklang bringen?

Dies war die Herausforderung, der sich das Computer-Center-Team der Universität Tunghai stellte. Die Universität hat sich das digitale Lernen zu eigen gemacht und einen intelligenten Campus aufgebaut, der Studenten und Mitarbeitern sowohl auf dem Campus als auch außerhalb des Campus kostenlosen drahtlosen Hochgeschwindigkeitsinternetzugang bietet. Zu Beginn jedes akademischen Jahres verbinden die neuen Studenten ihre Laptops mit dem Netzwerk der Universität.

Da die IT-Richtlinie jedoch keine Installation von Virenschutzprogrammen auf den Geräten der Studenten vorschrieb, waren viele der Laptops mit Malware infiziert. Diese kompromittierten Geräte führten zu Abstürzen von On- und Off-Campus-Netzwerken, zu einem übermäßigen Bandbreitenverbrauch und zu bösartigem Botnet-Traffic. Außerdem drang die Malware lateral in von der Universität verwaltete Computer ein. Daher erhielt die Universität Benachrichtigungen vom Regionalzentrum Taichung Network, dass das Netzwerk der Universität Tunghai angegriffen worden war und dass es ungewöhnliche Verbindungen herstellte.

„Das Rechenzentrum bot Schulungen zur Informationssicherheit an und forderte Studenten und Lehrkräfte auf, keine verdächtigen Links in E-Mails oder auf Webseiten anzuklicken“, erklärt Network Technology Director Chien-Hui Ou. „Die Angreifer entwickelten jedoch immer verschlagenerere Taktiken, die es Nutzern schwer machten, sofort zu erkennen, ob etwas legitim war. Dies führte letztendlich dazu, dass die Nutzer Opfer von Angriffen wurden.“



Universität Tunghai

Taichung, Taiwan
eng.thu.edu.tw

Branche

Öffentlicher Sektor

Lösung

[Secure Internet Access Enterprise](#)

Die wichtigsten Vorteile

- Verbesserte Sicherheit und kürzere Bearbeitungszeit bei Sicherheitsmanagement und Vorfallslösungen
- Proaktives Blockieren des Command-and-Control-Traffics von beeinträchtigten Geräten und Verringerung der lateralen Bewegung
- Reduzierung der Anzahl externer Sicherheitsbenachrichtigungen
- Optimiertes Sicherheitsbudget durch Verlagerung der Investitionen von Investitions- auf Betriebskosten



„Herkömmliche Antivirensoftware und Informationssicherheitslösungen, die auf der Analyse und Identifizierung von schädlichem Code basieren, greifen nicht rechtzeitig genug. Wenn eine neue Malware-Variante erscheint und Antiviren-Anbieter ihren Code und aktualisierte Signaturen noch nicht identifiziert haben, wird die Malware nicht erkannt“, sagt Kuang-Chin Chang von der Tunghai University Network Group. „Und aufgrund des Trends zur Verschlüsselung des Webtraffics nutzen Angreifer diese verschlüsselten Kanäle jetzt auch, um Angriffe zu starten. Zero-Day-Angriffe sind damit immer schwieriger zu stoppen.“

Akamai stoppt verdächtige Verbindungen effektiv

Das Team des Rechenzentrums erkannte, dass die Universität ihren bestehenden Sicherheitsansatz verbessern musste, und begann, Produkte in Erwägung zu ziehen, die DNS als Sicherheitskontrollpunkt nutzen. Dieser Ansatz sollte der Universität die Möglichkeit geben, ihre allgemeine Sicherheit zu verbessern, ohne dass die akademischen Freiheiten eingeschränkt werden.

Im Rahmen eines wettbewerbsorientierten Evaluierungsprozesses entschied sich die Universität für Akamai Secure Internet Access Enterprise als bevorzugte Lösung. Secure Internet Access Enterprise ist ein cloudbasierter Service, der ein Netzwerk und seine Nutzer proaktiv schützt, indem jede einzelne DNS-Anfrage analysiert wird. Jede Abfrage wird mit Echtzeit-Bedrohungsinformationen verglichen, die Akamai mit seiner unvergleichbaren Sicht auf den Internettraffic gesammelt hat. Dann erst wird der gewünschte Webinhalt blockiert oder zugelassen.

„Secure Internet Access Enterprise erkennt und blockiert DNS-Anfragen an Domains, die schädliche Inhalte wie Ransomware oder Coin-Mining-Malware übertragen oder Nutzerinformationen stehlen könnten“, so Chang. „Selbst wenn der Computer eines Studenten außerhalb des Campus mit Malware infiziert wird, kann die Malware keine externe Verbindung zum Command-and-Control-Server des Angreifers herstellen, sobald der Computer in das Campusnetzwerk zurückkehrt.“

Vor Secure Internet Access Enterprise war die Abwehr eines Informationssicherheitsvorfalls sehr aufwändig. Sobald ein Bericht über eine ungewöhnliche Verbindung empfangen wurde, mussten die Mitarbeiter des Netzwerkmanagements oftmals IP-Adressen verwenden, um den kompromittierten Computer aufzuspüren. Danach mussten sie Verbindungsdatensätze aus Protokolldateien finden, um den betroffenen Teilnehmer davon zu überzeugen, dass ein Vorfall aufgetreten ist, und anschließend den betroffenen Nutzer bitten, bei der Virusbereinigung zu kooperieren.

„Deshalb dauerte es meist etwa eine Woche, um einen Vorfall zu lösen. Und es nahm eine riesige Menge unserer Sicherheitsressourcen in Anspruch“, sagt Chang. „Seit der Einführung von Secure Internet Access Enterprise ist die Anzahl der gemeldeten Sicherheitsvorfälle enorm gesunken, und wir konnten unsere Ressourcen für andere Sicherheitsprojekte einsetzen.“

Chang fügt hinzu: „Secure Internet Access Enterprise kann besonders schnell und einfach installiert und konfiguriert werden. Darin unterscheidet es sich von den herkömmlichen Geräten, die zuerst vom Netzwerk getrennt und dann getestet werden müssen, bevor ein System in Betrieb gehen kann. Mit Secure Internet Access Enterprise leiten Sie Ihren DNS-Traffic einfach direkt auf die Plattform von Akamai. Der Vorgang ist schon nach wenigen Minuten abgeschlossen.“

Director Ou bemerkt dazu: „Secure Internet Access Enterprise liefert automatisch detaillierte Vorfallsberichte. Aus ihnen kann das Sicherheitsteam schnell erkennen, mit welcher Malware ein Computer infiziert wurde oder auf welche Weblinks vor der Infektion



Seit der Einführung von Secure Internet Access Enterprise ist die Anzahl der gemeldeten Sicherheitsvorfälle stark gesunken, und wir konnten unsere Ressourcen für andere Sicherheitsprojekte einsetzen.

Kuang-Chin Chang
Tunghai University Network Group

mit Coin-Mining-Malware geklickt wurde. Die Daten lassen sich in unsere SIEM-Lösung integrieren, sodass das Team die neuesten ungewöhnlichen Netzwerkaktivitäten besser verstehen kann, damit wir proaktiv reagieren können.“

Erhebliche Einsparungen bei Arbeit und Kosten

Chao-Tung Yang, Director, Electronic Computer Center, Universität Tunghai, betont die strategischen Vorteile. „Informationssicherheit ist heute wichtig und wird mit dem Wachstum digitaler Anwendungen in Zukunft immer wichtiger werden. Tunghai hat sich seit jeher dem Schutz von IT-Anwendungen und der Informationssicherheit verschrieben. Der Präsident unserer Universität unterstützt die Investitionen in die Informationssicherheit.“

Yang fährt fort: „Wenn man einen Schritt zurück geht und sich die aktuelle Wachstumsrichtung anschaut, ist klar, dass cloudbasierte Services keine vorübergehende Modeerscheinung sind. Frühere Verteidigungssysteme arbeiteten mit einer Kombination aus Software und Hardware und sie wurden verwaltet, indem Patches usw. aktualisiert wurden. Dies erforderte Zeit und Arbeit.“

Die cloudbasierten Services von Akamai bringen einen anderen Ansatz, mit dem der Wartungsaufwand insgesamt reduziert wird. Yang ist optimistisch, was die Zukunft der cloudbasierten Informationssicherheitsdienste angeht, und erklärt: „Es werden nicht nur die Arbeitskosten reduziert, sondern auch der Platzbedarf in Computerräumen sowie die Kosten für Klimaanlage und Strom. Dies entspricht dem Ziel des Rechenzentrums, den Energieverbrauch in Geräteräumen zu reduzieren.“

„Was die Kosten betrifft, so erfordert der Einsatz cloudbasierter Services im Gegensatz zum direkten Kauf physischer Geräte keinen großen einmaligen Investitionsaufwand“, so Yang. „Universitäten können sich Secure Internet Access Enterprise viel besser leisten, da die Lösung jährlich geleast wird.“

„Die Arbeit an der Informationssicherheit endet nie. Aber mit Secure Internet Access Enterprise wird der Arbeitsaufwand für das Vorfallsmanagement erheblich reduziert. Damit bleiben mehr Kapazitäten, um Abwehrmechanismen gegen Botnet-Angriffe zu stärken und Aktivitäten zu analysieren“, so Yang.



Secure Internet Access Enterprise kann besonders schnell und einfach installiert und konfiguriert werden. Darin unterscheidet es sich von den herkömmlichen Geräten, die zuerst vom Netzwerk getrennt und dann getestet werden müssen, bevor ein System in Betrieb gehen kann.

Kuang-Chin Chang
Tunghai University Network Group



Die Tunghai-Universität wurde 1955 gegründet und war die erste Privatuniversität in Taiwan. Die Universität ist die erste und einzige Bildungseinrichtung mit einem kompletten Bildungsprogramm vom Kindergarten bis zum PhD. Tunghai hat derzeit neun Colleges: College of Arts, College of Science, College of Engineering, College of Management, College of Social Sciences, College of Agriculture, College of Fine Arts and Creative Design, College of Law und International College. An der Tunghai-Universität studieren etwa 17.000 Studenten und sie beschäftigt fast 500 Lehrkräfte. <http://eng.thu.edu.tw/>.