r tec
cyber security

Branche: Medienunternehmen

Konzept: Malwareschutzkonzept

No.: 06

SUCCESS STORIES

Malwareschutzkonzept

MALWARESCHUTZKONZEPT.

Medienunternehmen.
Einfallstore identifizieren. Angriffe abwehren.

Alle Fakten auf einen Blick:

Aufgabe

- Review der gesamten IT-Security Infrastruktur
- Entwicklung eines Diagramms zur Nachverfolgung des Datenflusses und der dort eingesetzten Schutzmechanismen zur Malware-Abwehr sowie deren Analyse, ausgehend von verschiedenen Angriffsvektoren (E-Mail, Web, USB-Datenträger etc.) sowie Angreifern von innen und außen
- Identifizierung von Handlungsfeldern und Entwicklung konkreter Handlungsempfehlungen zur Erhöhung des IT-Security Reifegrads
- Aufzeigen möglicher Zusammenarbeit bestehender IT-Security Komponenten verschiedener Hersteller

Vorgehen

- Workshop zur Informationsaufnahme und Zielsetzung
  - Erfassen bestehender IT-Security Lösungen und Festlegen der zu berücksichtigenden Komponenten
  - Erfassen vorhandener reputationsbildender Systeme und Erstellung einer Reputationsmatrix
  - Bestimmung relevanter Bedrohungen und Angriffsszenarien
- Erstellung des Malwareschutzkonzepts
- Ergebnispräsentation – Vorstellung des entwickelten Konzepts und Beantwortung von Rückfragen

Projektziele

- Angriffsstrategie gegen gängige Angriffsszenarien entwickeln wie z. B.:
  - Phishing/Social Engineering (E-Mail, Wechseldatenträger)
  - Kompromittierte Webseite (»Drive-by Download«, Browser-Exploit)
  - Kompromittierung von DMZ-Systemen
  - Physischer Zugriff (Netzwerkbuchse in Konferenzraum)
- Mögliche Integrationen vorhandener Infrastruktur in DXL und OpenDXL und TIE Server
- Entwicklung automatischer Reaktionen bei Malwarefund (wie Firewall-Blockregel oder Fullscan auf dem Endpoint etc.)
- Entscheidungsvorlage für die Risikostrategie sowie Investitions- und Ressourcenplanung

Ergebnisse

- Entwicklung von herstellerübergreifenden Kombinationen und Technologiestrategien gegen Angriffsvektoren auf der Basis der ermittelten Angriffsszenarien
- Identifikation von Optimierungspotenzial innerhalb der bestehenden IT-Security Landschaft
- Handlungsempfehlungen für den Einsatz von zusätzlichen Technologien und Anpassung bestehender Security-Komponenten
- Cyber Security Plan – Arbeitspakete und Priorisierung für effiziente Umsetzung in Zeithorizonten
- Management Summary für die Risikostrategie sowie Investitions- und Ressourcenplanung
- Ausblick auf automatisierte Abwehr von Cyberangriffen bzw. Reduzierung der Angriffsvektoren

Die erfolgreiche Umsetzung des Projekts hat mich befähigt, interne Prozesse anzustoßen, die uns sicherheitstechnisch auf ein neues Niveau bringen.

Teamleiter IT-Security

Malwareschutz als Grundlage für Integrität, Kontinuität und Verfügbarkeit von Medieninhalten

Bereits im Jahr 2018 warnte das Bundesamt für Verfassungsschutz (BfV) vor »besonders hochwertigen Cyberangriffen« auf deutsche Medienhäuser. Das BfV sprach von Angriffen mit mutmaßlich »nachrichtendienstlichem Hintergrund« und warnte vor einer Phishing-Mail-Welle.

Cyberspionage stellt für Medienunternehmen nicht unbedingt die vorrangige Herausforderung dar, entscheidende Fragen sind aber wie stellen wir sicher, dass die Nachrichten auch »unsere Nachrichten« sind? Wie stellen wir sicher, dass wir kontinuierlich senden können?

Auch wenn das IT-Sicherheitsgesetz 2.0 noch nicht beschlossen ist, sieht der Referentenentwurf für das »IT-Sicherheitsgesetz 2.0« (IT-SiG 2.0) zukünftig eine Meldepflicht über Sicherheitsvorfälle vor. Zudem ist geplant, die Meldepflichten auf weitere Bereiche der Wirtschaft auszudehnen, bei denen ein besonderes öffentliches Interesse vorliegt. Dies betrifft unter anderem auch Medienunternehmen.

Ziel des hier anonymisiert beschriebenen Projekts war es daher, für ein großes Medienunternehmen in Köln eine fundierte Analyse der vorhandenen IT-Security-Infrastruktur zu erstellen und eine Angriffsstrategie gegen die gängigen Angriffsszenarien zu entwickeln.

Die Herausforderung bestand hier darin, zunächst einmal die entscheidenden Angriffsvektoren zu identifizieren, herstellerübergreifende Technologiestrategien zu entwickeln und nach Möglichkeit eine Automatisierung der Angriffsreaktion zu etablieren.

Für das auftraggebende Medienunternehmen war dies bereits das Projekt 2.0, der bisherige Dienstleister war gescheitert.

Wesentlicher Erfolgsfaktor hier: Die r-tec IT Security GmbH verfügt über ein breites Portfolio und konnte sich der Aufgabe daher abteilungsübergreifend mit einem Team aus IT Security Consultant, Architect und Engineering, Professional Service und Vulnerability Management stellen.

»Für uns hat sich hier eine vertrauensvolle Zusammenarbeit auf Augenhöhe entwickelt, wir sind sehr zufrieden mit der fachlichen und organisatorischen Expertise der Mitarbeiter und des Unternehmens«, äußerte sich der interne Projektleiter. »Supergut« und entscheidend für die schnelle Umsetzung des Projekts war »das Ressourcenmanagement der r-tec, das haben wir so noch nicht kennengelernt. Wir müssen flexibel mit internen Zeitressourcen umgehen, das bedeutete bei anderen Dienstleistern, dass Termine mitunter ein halbes Jahr Vorlauf hatten. So kommt man nicht zu Ergebnissen.«

Der Zeitrahmen des Projekts betrug fünf Monate, vom initialen Workshop im April 2019 über die Entwicklung des Malwareschutzkonzepts bis zum erfolgreichen Abschluss im September 2019 mit der Vorstellung des Cyber Security Plans und der Vorlage einer Management Summary als Entscheidungsvorlage für die Risikostrategie sowie Investitions- und Ressourcenplanung. ■

Die r-tec IT Security GmbH, mit Sitz in Wuppertal, wurde 1996 von Dr. Stefan Rummenhöller gegründet. Als Wegbereiter und Wegbegleiter schaffen wir für unsere Kunden sichere Räume für die Entwicklung ihrer Organisationen und die Verwirklichung ihrer Visionen. Unsere Kunden aus dem gehobenen Mittelstand, Konzerne, kommunale Rechenzentren und Bundes- oder Landesbehörden vertrauen seit über 20 Jahren auf unsere hoch spezialisierten Experten.

Als Strategic Supplier für Cyber Security Services schützen wir die Werte unserer Kunden vor Bedrohungen und begleiten ihr Security Management von der Initiierung über die Einführung bis zum Betrieb auf allen Ebenen.

Wir leben Regeltreue, höchste Qualitätsstandards und Servicementalität. Unser Unternehmen haben wir nach den Strukturen und Richtlinien der DIN ISO 9001:2015 und der ITIL aufgebaut. Wir sind nach ISO 27001 zertifiziert.

r-tec IT Security GmbH | Hatzfelder Str. 167 | 42281 Wuppertal
www.r-tec.net | +49 (0) 202 31767–100