REDGUARD
SECURING YOUR ASSETS

SIMULIERTER ANGRIFF AUF EINE GEMEINDE

Sicherheit geht jede Organisation etwas an. Die Gemeinde Vilters-Wangs folgte dieser Devise und liess in einem umfassenden Penetration Test und einem vorgängigen Sicherheitsaudit ihre Umgebung auf mögliche Schwachstellen hin überprüfen. Für eine Gemeinde ungewöhnlich? Überhaupt nicht! Durch das Endergebnis konnte zwischenzeitlich bereits viel bewirkt werden und in Form von Penetration Tests wird festgestellt, wie sicher eine Organisation aufgebaut ist. Kritische Daten sind überall vorhanden und abfangbar.

Technische Betriebe Vilters-Wangs
Elektrizität | Kommunikation | Wasser

Das Elektrizitätswerk Vilters-Wangs betreibt zwei verschiedene Netzwerke zur Steuerung der Produktionsanlage (EW-Leitsystem) und zum Auslesen der verteilten Stromzähler. Im Rahmen eines Sicherheitsaudits wurde überprüft, wie gut das Netzwerk gegen digitale Angriffe geschützt ist. Dazu wurde in einer ersten Phase die Architektur analysiert und auf konzeptionelle Schwachstellen untersucht. In einer zweiten Phase wurde das Netzwerk diversen technischen Tests unterzogen. Die Security-Tester von Redguard ermittelten, ob sich ein Angreifer über das Internet oder über die Stromzähler unerlaubten Zugang zum Netzwerk verschaffen könnte. In diesem Rahmen wurden unter anderem auch Vektoren wie Social Engineering und Bedrohungen durch die Mitarbeiter des IT-Dienstleisters berücksichtigt. Zudem verifizierte Redguard, ob die konzeptionelle Architektur der Netzwerk-Zonierung der Realität entspricht.

Schwerpunkte definieren

Vor Beginn des Sicherheitsaudits wurde in einem ersten gemeinsamen Kickoff Meeting zwischen beiden Parteien eine Übersicht über die Systeme und Netzwerke gegeben sowie der genaue Scope definiert. Durch diese Definition wird ein möglichst effizientes Arbeiten ermöglicht, denn die Schwerpunkte sind klar definiert und die vorgegebene Zeit kann gezielt eingesetzt werden. In einem weiteren Schritt haben die Security-Tester von Redguard einen Architektur-Review über die beiden Netzwerke durchgeführt. Diese Überprüfung wird – wie in diesem Fall – oft auch als Ergänzung zu einem technischen Penetration Test beigezogen, um einen konzeptionellen Review des Ist-Zustandes zu machen, und half dabei, Schwerpunkte für den Penetration Test zu setzen. Die Gemeinde Vilters-Wangs hat sich dementsprechend für das Gesamtpaket entschieden und sowohl den Architektur-Review als auch den Netzwerk-Penetration-Test bestellt. Der Architektur-Review zeigt auch Schwachstellen auf, die durch einen reinen Penetration Test eventuell nicht zu identifizieren sind, wie zum Beispiel Schwächen in logischen Prozessen oder im Zusammenspiel mit anderen Komponenten. Dies geschieht durch das Dokumentenstudium, in welchem beispielsweise Betriebskonzepte, das Systemdesign sowie die Netzwerkzonierung in Bezug auf Best Practices analysiert und etwaige Schwachstellen identifiziert werden.

Als Vertiefung und Verifikation der ermittelten Informationen werden gemeinsam mit den involvierten Fachspezialisten Interviews geführt. Das Endresultat richtet sich somit nach einer Systemprüfung auf konzeptioneller Ebene aus.

Klassischer Penetration Test

Durch aktive, sowohl automatisierte als auch manuelle Angriffe wurden die vordefinierten Zielsysteme durch die Sicherheitsexperten der Redguard überprüft. Die automatisierten Angriffe helfen dabei, die sogenannten “Low hanging fruits”, also einfach zu entdeckende Schwachstellen, zu finden. Manuell ausgeführte Angriffe können durch die Erfahrung der Security-Tester komplexere Systemzusammenhänge abdecken und Angriffspfade untersuchen, wozu automatisierte Tools nicht fähig sind. Es konnten somit nicht nur offensichtliche, sondern auch tiefgehende und komplexe Schwachstellen in den Systemen frühzeitig erkannt werden.

Das Sicherheitsaudit der Gemeinde Vilters-Wangs wurde in zwei Teilen durchgeführt. Im ersten Teil wurde das Netzwerk der Gemeinde auf verwundbare Services hin geprüft. Hier versuchten die Security Tester von Redguard, sich über verschiedene Wege einen Zugang zum Netzwerk zu verschaffen. Dies beinhaltete Tests aus dem Internet, den Räumlichkeiten des IT-Dienstleisters wie auch eine direkte Anbindung an die Serverzone und das SmartMeter-Netz. Dazu wurde den Security-Testern Zugang zu einer produktiven Smart-Meter-Anlage eines Wohnblocks gegeben. So konnten der Netzwerkverkehr zwischen den SmartMetern und den Datensammlern abgefangen und die verwendeten Netzwerkprotokolle analysiert werden.

In einem zweiten Teil wurde untersucht, ob die Netzwerk-Konfiguration der offiziellen Systemarchitektur entspricht. Dafür waren die Security-Tester vor Ort im internen Netzwerk,

„Sämtliche Erwartungen betreffend dem Security Audit wurden voll und ganz erfüllt. Der entstandene Bericht dient nun als Grundlage zur Verbesserung der Informationssicherheit.”

Patrik Schlegel, Gemeinderatsschreiber

um so beispielsweise zu überprüfen, ob die Zonierung korrekt umgesetzt wurde. Dies war besonders wichtig, da sichergestellt werden musste, dass die SmartMeter keinen Weg hatten, das Leitsystem der Gemeinde oder andere Smart-Meter zu erreichen. Sämtliche gefundene Findings wurden anschliessend in einem umfassenden Bericht festgehalten und der Gemeinde Vilters-Wangs übergeben. Dieser Bericht dient der Gemeinde als Grundlage zur Verbesserung ihrer Systeme.

Zusammenarbeit mit Redguard

„Die Erwartungen an die Mitarbeitenden der Redguard wurden voll und ganz erfüllt“, so Patrik Schlegel, Gemeinderatsschreiber der Gemeinde. Die Gemeinde Vilters-Wangs hatte sich im Vorfeld noch nie mit einer Auditierung auseinandergesetzt, weshalb sämtliche Erfahrungen in diesem Bereich fehlten. Schlegel weiter: „Die Zusammenarbeit hat deshalb so gut funktioniert, weil die Security-Tester von Redguard sämtliche Anliegen und Fragen rund um die Auditierung fachkompetent erklärt haben.“ Die Fachexpertise von Redguard sei sowohl für grössere wie auch für kleinere Gemeinden eine gute Lösung, um die interne Infrastruktur zu testen. Schlegel: „Redguard ist als Partner geeignet, da individuell auf Bedürfnisse eingegangen wird. Die Kommunikation war während der gesamten Projektdauer einwandfrei und das Know-how wurde gezielt eingesetzt. Das Endresultat, der sogenannte Bericht, kommt in einer systematischen Darstellung daher, die Priorisierungen sind allesamt erklärt und dieses Resultat dient als Grundlage zur Weiterbearbeitung und Sicherung der Schwachstellen.“

Erstelldatum 02/2019, RG-C0