LINK Institut für Markt- und Sozialforschung. Seit 1996 ist bw digitronik der IT-Security Partner.

Jürg Tütsch,
Mitglied VR/GL, Leiter Produktion

LINK Institut

IT-Security Lösungen
- McAfee Endpoint Protection Suite und Host Intrusion Prevention
- Dell SonicWALL Firewalls
- Clearswift E-Mail/Anti-Spam Gateway
- Symantec-PGP E-Mail Encryption/NetShare/ Command Line
- Totemo totemodata (sicherer Datenaustausch)

Dienstleistungen
- bw digitronik Security Engineering für alle verwendeten Lösungen
- bw digitronik Security Awareness Consulting und Training
- bw digitronik Security Consulting (Policies, Konzepte, Second Opinion)

Background

Das LINK Institut für Markt- und Sozialforschung wurde 1981 gegründet und ist heute das grösste unabhängige Umfrage-Forschungsinstitut im DACH-Markt. Mit etwas über 800 Mitarbeitenden an den Standorten Zürich, Luzern, Lausanne, Lugano und Frankfurt ist das Unternehmen im Heimmarkt Schweiz in allen Sprachregionen vertreten und international ausgerichtet. Durch die langjährige Erfahrung hat sich das LINK Institut umfassende Methodenkompetenz und vertiefte Branchenkenntnis erarbeitet. Durch die hohe Qualität der Datenerhebung ergibt sich eine einzigartige Ergebnisqualität, sodass die Kunden eine fundierte und fokussierte Entscheidungsgrundlage erhalten. Die Kernkompetenz des LINK Instituts liegt auf der Umfrageforschung mit den Komponenten Studiendesign, Datenerhebung, Auswertung und Analytics. Link verfügt als eines der wenigen Institute über ein proprietäres System für computergestützte Umfragen.

Durch permanente Innovation und Qualität hat das LINK Institut in den vergangen 30 Jahren eine führende Stellung im Markt gewonnen. Bereits 1984 war LINK der Schweizer Pionier in der computergestützten Telefonbefragung mit dem eigenen CATI-System «TIP». 1998 profilierte sich LINK bei der Einführung des zu 100 Prozent rekrutierten LINK Internet Panels als First Mover in der Online-Forschung. 2006 wurden die Online-Fokus-Gruppen und Blogs eingeführt. Seit 2011 setzt LINK auf Mobile Research. Das heisst, LINK befragt einerseits neu auch über Smartphones, und erreicht anderseits dank Mobile RDD auch Personen, die nicht mehr über einen eingetragenen Festnetzanschluss verfügen. Viele Kunden vertrauen darauf, dass LINK die am besten geeignete, technologisch führende Methode für die Lösung ihrer Informationsbedürfnisse einsetzt.

Ausgangslage

Das LINK Institut ist in den letzten Jahren stetig gewachsen und die Anforderungen in den Bereichen Sicherheit, Datenschutz und Compliance wurden erhöht. Auch das IT-Team wurde verstärkt und ausgebaut. Für die Erhebungen beschäftigt das Unternehmen viele Teilzeitmitarbeitende an diversen Standorten, die Daten verarbeiten. Da die meisten Prozesse IT-unterstützt ablaufen, ist es zentral, dass die Mitarbeitenden den richtigen Umgang mit der IT kennen und die vertraulichen Daten entsprechend schützen. Datensicherheit und hohe Vertraulichkeit gehören zu den Kernthemen der IT-Security beim LINK Institut.

IT-Sicherheit und Datenschutz beim LINK Institut

Wie bei den meisten Unternehmen in den 1990er-Jahren begann auch beim LINK Institut die IT-Security mit der Anschaffung einer Virenschutzlizenz von McAfee. Bis heute dient die McAfee Endpoint Protection für den zuverlässigen Schutz der Clients und Server vor Malware und anderen unerwünschten Programmen. Die mobilen Rechner werden zusätzlich mit McAfee Host Intrusion Prevention geschützt. Als zentrales Verwaltungs- und Reporting-Tool ist der McAfee ePolicy Orchestrator im Einsatz. Damit können alle angeschlossenen Endgeräte überwacht, aktualisiert, umkonfiguriert und mit neuen Richtlinien ausgestattet werden. Mit der umfassenden Reporting-Funktion können die gewünschten Übersichten erstellt werden, und der Administrator ist in Echtzeit auf dem aktuellen Stand. bw digitronik bietet für diesen Hersteller einen 7x24-Support, damit keine wichtigen Fragen unbeantwortet bleiben und die Verfügbarkeit des Schutzes sichergestellt werden kann.

In einem weiteren Schritt wurde dann ein Managed Firewall Service in Betrieb genommen, der mit SonicWALL-Hardware betrieben wurde. Heute sind sämtliche Standorte mit Dell SonicWALL Appliances ausgestattet, um auch die sichere Kommunikation innerhalb des Unternehmens zu gewährleisten. Die aktuellen Next Generation Firewall-Modelle sind ausgerüstet mit modernsten Security-Services und können Applikationen (Layer 7) gezielt analysieren, blockieren oder nur Teile davon deaktivieren (z. B. Games bei FaceBook).

Um am Netzwerk-Perimeter zusätzliche Content Filtering-Funktionen zu erhalten, wurde die bewährte Clearswift E-Mail- und Anti-Spam-Lösung eingeführt. Diese filtert mit hoher Genauigkeit und in sehr guter Performance die unerwünschten E-Mails bereits am Gateway heraus, damit diese unnötige Datenflut die interne Mailinfrastruktur nicht zusätzlich belastet. Die umfassenden Content Filtering-Funktionen von Clearswift können E-Mails und Anhänge genau analysieren und zerlegen, sodass auch mehrfach verschachtelte Dateien überprüft werden können. Für die Benutzer steht ein komfortabler und einfach bedienbarer Dienst zur Verfügung,

www.link.ch
www.bwdigitronik.ch/securitysolutions

um die gefilterten E-Mails bei Bedarf zu kontrollieren und die seltenen falsch blockierten Nachrichten freizuschalten.

Zwischendurch hat bw digitronik gemeinsam mit dem LINK Institut die «Acceptable Use»-Richtlinie aktualisiert und für die IT-Strategie des Unternehmens die «TOP-Level-Security»-Policy verfasst. Dies waren wichtige Grundlagen für die sich weiter entwickelnde IT-Security-Strategie und für die IT-Security Awareness.

Um die Daten des Unternehmens auf verschiedene Arten zu verschlüsseln, wurden Lösungen von Symantec-PGP implementiert. Vertrauliche E-Mails werden nun mit dem PGP Universal Gateway verschlüsselt übermittelt. Und wenn verschiedene Personen an einem Projekt arbeiten und vertrauliche Daten gemeinsam nutzen, werden sie von PGP NetShare unterstützt. Für die sichere interne Datenübertragung wird PGP Command Line eingesetzt. Da auch die vertraulichen Daten immer grösser werden und diese zum Teil nicht mehr auf dem E-Mail-Weg verschickt werden können, wurde zuletzt die Schweizer Lösung totemodata für den sicheren File Transfer installiert. Diese ermöglicht es dem LINK Institut, grosse Files einfach und sicher verschlüsselt auszutauschen, ohne dass der Partner eine Verschlüsselungslösung im Einsatz haben muss.
Aktuell durfte bw digitronik ein Konzept für das Incident Management und für das Training im Bereich IT-Security Awareness für das LINK Institut erarbeiten. Beide Unternehmen sind gemeinsam an den neuen Herausforderungen gewachsen und entwickeln sich weiter.

Spannende und erfolgreiche Partnerschaft seit über 17 Jahren

Jürg Tütsch, Leiter Produktion und Miteigentümer des LINK Instituts, freut sich: «Wir haben mit verschiedenen IT-Security-Experten der bw digitronik zu tun und es ist eine erfreuliche Zusammenarbeit. Wir werden sympathisch und mit gesundem Menschenverstand beraten.» Die beiden Unternehmen können auf eine über 17-jährige spannende Zusammenarbeit zurückblicken. bw digitronik unterstützt die Geschäftsleitung und das IT-Team vom LINK Institut engagiert und kompetent in den Bereichen IT-Security Consulting, Engineering, Awareness und der Auswahl und dem Betrieb von IT-Security Lösungen. So handeln die Mitarbeitenden nach sinnvollen Richtlinien und die Kundendaten sind sicher geschützt vor unerlaubtem Zugriff.

McAfee Host Intrusion Prevention: Präventiver Schutz für Endgeräte, Daten und Anwendungen.

Die Herausforderung: Die Verwaltung der Sicherheit und die Steuerung der Internetverbindung für Desktops, Laptops und Servern kann in Unternehmen grosse Probleme bereiten. Aufgrund der wachsenden Anzahl von aktiven profitorientierten Internetkriminellen gab es in den letzten Jahren immer mehr neue Bedrohungen. IT-Sicherheitsteams stehen unter immensem Druck, alle Endgeräte vor der schnell zunehmenden Anzahl komplexer Bedrohungen zu schützen. Und da mehr als 32 Prozent der Angriffe innerhalb von drei Tagen nach Entdeckung der betreffenden Schwachstelle erfolgen, sind Unternehmen gefährdet, denn bis zur Implementierung der Endgeräte-Patches können dreissig oder mehr Tage vergehen. Unternehmen benötigen Schutz vor Zero-Day-Bedrohungen, um die Sicherheit und Zeit für die ordnungsgemässe Priorisierung, Planung, Erprobung und Implementierung von Patches zu erhalten.
Eine der grössten Herausforderungen für IT-Manager besteht darin, unternehmenskritische Endgeräte erfolgreich vor bekannten und unbekannten Angriffen zu schützen, bevor diese Schaden anrichten. Virenschutz allein reicht nicht aus, da Angriffe auf Schwachstellen schneller erfolgen und immer komplexer werden. Die Lösung besteht darin, eine präventive Sicherheitsstrategie zu implementieren, die verhindert, dass Angriffe überhaupt stattfinden. Mit einem präventiven Sicherheitsansatz für Endgeräte können IT-Manager sicherstellen, dass alle Endgeräte und vertraulichen Daten geschützt sind und die Geschäftskontinuität aufrechterhalten wird.

McAfee Host Intrusion Prevention für Endgeräte: Als integraler Bestandteil von McAfee Total Protection (ToPS) for Endpoint schützt McAfee Host Intrusion Prevention (Host IPS) Endgeräte vor bekannten und Zero-Day-Bedrohungen durch die Kombination von Signatur und verhaltensorientiertem Intrusion Prevention-Schutz mit einer zustandsgesteuerten Desktop Firewall und Anwendungskontrolle. McAfee Host IPS reduziert die Häufigkeit und Dringlichkeit von Patches, erhält die Geschäftstätigkeit und Mitarbeiterproduktivität, schützt die Vertraulichkeit von Daten und vereinfacht die Einhaltung von gesetzlichen Bestimmungen.

Verwaltbarkeit für Unternehmen: McAfee ePolicy Orchestrator (ePO) ist die branchenführende Plattform für die Verwaltung der Systemsicherheit, die Unternehmen einen koordinierten, präventiven Schutz vor Bedrohungen und Angriffen bietet. Mit ePO als Kern der McAfee-Lösungen für das Sicherheitsrisiko-Management (SRM) können Administratoren von einer zentralen, webbasierten Konsole aus rund um die Uhr das Risiko unberechtigter regelwidriger Systeme mindern, den Schutz aktuell halten, Sicherheitsrichtlinien einrichten und durchsetzen sowie den Schutzstatus überwachen. Implementieren Sie ePO und verwalten Sie Ihre gesamten neuen Sicherheitslösungen oder erweitern Sie Ihre Investitionen in unternehmensorientierte Lösungen für Sicherheitsmanagement und integrieren Sie Host IPS in Ihre bestehende ePO-Infrastruktur. Mit einem einzigen Agenten lässt sich die Endgerätesicherheit leicht bereitstellen, konfigurieren und verwalten. Die Konsolidierung des Sicherheitsmanagements bedeutet nicht nur weniger Probleme, sondern ebenfalls erhebliche IT-Kosteneinsparungen.

McAfee Host IPS ist ein integraler Bestandteil von McAfee ToPS for Endpoint, McAfees umfassender Sicherheitslösung für Endgeräte. ToPS for Endpoint ist vollständig in McAfee ePO, die zentrale SRMPlattform, integriert, die den Unternehmen durch unerreichte betriebliche Effizienz Zeit und Geld spart.

McAfee®
An Intel Company

www.mcafee.com/de/products/host-ips-for-desktop.aspx
www.mcafee.com/de/products/host-ips-for-server.aspx