

Firewall-Sicherheit beginnt mit dem laufenden Betrieb

19.10.2026, 10:09 | IT, New Media & Software

Pressemitteilung von: *NetWyl Informatik GmbH*



Eine Firewall schützt nicht automatisch dauerhaft. Regeln, Updates, Logs und Störungen müssen laufend betreut werden. Warum der Betrieb entscheidend ist - und wo Unternehmen Unterstützung brauchen.

Luzern, Oktober 2026 - Eine Firewall gehört für Unternehmen zur Grundausrüstung der IT-Sicherheit. Doch mit der Installation allein ist ihre Aufgabe nicht erfüllt. Regeln müssen angepasst, Updates eingespielt, Logs geprüft und Auffälligkeiten bewertet werden. Gleichzeitig verändern sich Netzwerke, Anwendungen und Zugriffsanforderungen laufend. Für viele Unternehmen entsteht damit eine unsichtbare Aufgabe: Die Infrastruktur muss permanent gepflegt werden, obwohl im Tagesgeschäft oft andere Themen dringender erscheinen.

NetWyl Informatik aus Luzern erlebt in der Praxis, dass genau an dieser Stelle Sicherheitslücken entstehen können. Nicht unbedingt, weil Unternehmen keine geeignete Firewall besitzen, sondern weil für den laufenden Betrieb die Zeit oder eine klare Zuständigkeit fehlt. Firewall- und Netzwerk-Sicherheit wird damit weniger zu einer einmaligen technischen Anschaffung als zu einer dauerhaften organisatorischen Aufgabe.

Wenn Regeln liegen bleiben

Eine Firewall ist kein System, das einmal eingerichtet wird und anschliessend unverändert funktioniert.

Neue Anwendungen benötigen Zugriffe. Mitarbeitende wechseln Rollen. Standorte werden angebunden, Cloud-Dienste kommen hinzu und bestehende Systeme werden ersetzt. Entsprechend verändern sich auch die Anforderungen an Netzwerkregeln.

Auf der NetWyl-Leistungsseite wird genau dieses Spannungsfeld beschrieben: Regeln verändern sich, Updates häufen sich und gleichzeitig wachsen die Log-Daten. Im Alltag fehlt internen IT-Teams jedoch häufig die Zeit, alles kontinuierlich im Blick zu behalten.

Das kann zu einem schleichenden Problem werden. Eine Regel wird für einen kurzfristigen Bedarf eingerichtet und später nicht mehr überprüft. Ein Wartungsfenster wird verschoben. Ein Log-Eintrag wird zwar erzeugt, aber nicht ausgewertet. Eine Anpassung funktioniert technisch, wird aber nicht ausreichend dokumentiert.

Jede dieser Situationen mag für sich genommen unkritisch erscheinen. In ihrer Summe kann daraus jedoch eine Infrastruktur entstehen, die schwieriger zu überblicken und zu betreiben ist.

Erfahren Sie mehr über das Thema: <https://www.netwyl-informatik.ch/leistungen/betrieb-und-support-von-firewalls-und-infrastrukturen/>

Sicherheit ist kein Zustand, sondern ein Prozess

Für Piotr Kusak von Wyl, Gründer von NetWyl Informatik, steht deshalb nicht nur die technische Lösung im Vordergrund.

"Wir sorgen mit massgeschneiderter IT-Security und persönlicher Betreuung für eine sichere Basis, damit Ihr Unternehmen sorgenfrei wachsen und innovieren kann."

Der Gedanke dahinter ist auch für den Betrieb von Firewalls relevant. Eine sichere Infrastruktur muss nicht nur funktionieren, wenn sie eingerichtet wird. Sie muss sich an neue Anforderungen anpassen können, ohne dass dabei Sicherheits- und Betriebsrisiken aus dem Blick geraten.

NetWyl beschreibt den eigenen Ansatz deshalb als laufenden Prozess aus Review, Konzept, Betrieb und Optimierung. Dazu gehören unter anderem Firewall-Änderungen, Regel-Reviews, Log- und Threat-Analysen sowie Fehleranalyse und Störungsbehebung.

Das klingt weniger spektakulär als ein neuer Security-Ansatz. Für den Alltag eines Unternehmens ist es jedoch gerade diese kontinuierliche Arbeit, die darüber entscheidet, ob eine Infrastruktur langfristig übersichtlich und belastbar bleibt.

Eine Firewall produziert Arbeit

In der öffentlichen Wahrnehmung wird eine Firewall häufig als Schutzschild zwischen dem Unternehmen und dem Internet verstanden. Technisch ist sie weit mehr als das.

Sie bildet einen zentralen Kontrollpunkt für Netzwerkverbindungen und Zugriffe. Damit entstehen gleichzeitig zahlreiche Informationen und administrative Aufgaben.

- Welche Verbindungen sind erlaubt?
- Welche Regeln werden tatsächlich noch benötigt?
- Welche Zugriffe sind nur vorübergehend eingerichtet worden?
- Welche Systeme kommunizieren miteinander?
- Welche Auffälligkeiten tauchen in den Logs auf?
- Und welche Änderungen müssen dokumentiert werden?

Je komplexer die Infrastruktur, desto schwieriger wird es, diese Fragen nebenbei zu beantworten.

Genau deshalb kann eine Firewall paradoxerweise selbst zum organisatorischen Engpass werden. Nicht weil sie schlecht funktioniert, sondern weil ihr Betrieb Fachwissen und kontinuierliche Aufmerksamkeit benötigt.

Regel-Wildwuchs ist ein Sicherheits- und Betriebsproblem

Besonders relevant ist dabei das Regelmanagement.

In gewachsenen Netzwerken entstehen Firewall-Regeln häufig über Jahre. Unterschiedliche Mitarbeitende oder externe Dienstleister nehmen Anpassungen vor. Anwendungen werden eingeführt und später ersetzt. Temporäre Ausnahmen

bleiben bestehen. Zuständigkeiten verändern sich.

Mit der Zeit kann daraus ein Regelwerk entstehen, das zwar funktioniert, aber nur noch schwer nachvollziehbar ist.

NetWyl nennt deshalb Regel-Reviews und Optimierung als eigenen Bestandteil des Firewall-Betriebs. Bestehende Policies sollen überprüft, strukturiert und dokumentiert werden. Ziel ist, nachvollziehbare Regeln zu schaffen und unnötigen Wildwuchs zu vermeiden.

Das hat nicht nur einen Sicherheitsvorteil.

Auch bei einer Störung kann eine saubere Struktur entscheidend sein. Wenn klar dokumentiert ist, weshalb eine Regel existiert und welche Systeme davon betroffen sind, lässt sich eine Änderung schneller nachvollziehen. Das erleichtert die Fehlersuche und reduziert das Risiko, bei einer Anpassung unbeabsichtigt andere Geschäftsprozesse zu beeinträchtigen.

Logs allein schaffen noch keinen Überblick

Ein ähnliches Problem entsteht bei der Überwachung.

Moderne Firewalls können grosse Mengen an Ereignissen protokollieren. Die technische Möglichkeit, Daten zu sammeln, bedeutet allerdings noch nicht, dass daraus automatisch ein Sicherheitsgewinn entsteht.

Jemand muss relevante Ereignisse erkennen und einordnen.

NetWyl beschreibt deshalb Log- und Threat-Analysen als Teil des laufenden Betriebs. Auffälligkeiten sollen erkannt und entsprechende Massnahmen eingeleitet werden. Wie häufig Logs geprüft werden, kann laut NetWyl je nach Vereinbarung von täglich bis wöchentlich reichen; bei Auffälligkeiten erfolgt eine Benachrichtigung.

Das verdeutlicht einen grundsätzlichen Unterschied zwischen Monitoring und echtem Sicherheitsbetrieb.

Monitoring erzeugt Informationen.

Security-Betrieb sorgt dafür, dass aus diesen Informationen Entscheidungen und Massnahmen entstehen.

Wenn die interne IT andere Prioritäten hat

Für interne IT-Abteilungen stellt sich dabei ein praktisches Problem.

Die Firewall ist wichtig. Die Netzwerkumgebung muss funktionieren. Sicherheitsupdates dürfen nicht beliebig aufgeschoben werden. Gleichzeitig warten Projekte, Benutzeranfragen, Migrationen und andere betriebliche Aufgaben.

Ein IT-Team kann daher durchaus wissen, dass ein Regel-Review oder eine Log-Analyse notwendig wäre und diese Aufgabe trotzdem verschieben müssen.

Auf der NetWyl-Seite wird dieses Spannungsfeld ausdrücklich angesprochen: Interne IT-Teams seien häufig ausgelastet, wodurch Änderungen liegen bleiben und Wartungsfenster verschoben werden können. Ohne dedizierte Betreuung könnten Risiken dadurch schleichend wachsen.

Das Problem ist damit nicht zwingend fehlende Kompetenz.

Es ist fehlende Kapazität.

Diese Unterscheidung ist wichtig, weil sie eine andere Form der Unterstützung nahelegt. Unternehmen benötigen nicht

unbedingt eine neue Firewall. In manchen Fällen benötigen sie vor allem jemanden, der den Betrieb der bestehenden Infrastruktur zuverlässig übernimmt.

Hier gelangen Sie zu den Leistungen der Netwyl Informatik GmbH: <https://www.netwyl-informatik.ch/leistungen/>

Unterstützung muss nicht gleich Outsourcing bedeuten

Eine vollständige Auslagerung der IT ist für viele Unternehmen weder notwendig noch gewünscht.

Interne IT-Teams kennen die Geschäftsprozesse, Anwendungen und Nutzer. Sie sollten deshalb auch weiterhin eine zentrale Rolle spielen. Externe Unterstützung kann dort ansetzen, wo spezialisierte Aufgaben oder laufende Betriebsarbeit zusätzliche Kapazität benötigen.

NetWyl bietet dafür unterschiedliche Modelle an: vom Quick-Check über die Optimierung bestehender Firewall- und Netzwerkstrukturen bis zur laufenden Betriebsübernahme. Auch eine zeitlich begrenzte Ferienvertretung gehört zum beschriebenen Leistungsumfang.

Gerade die Ferienvertretung zeigt, dass es nicht immer um eine grundsätzliche Make-or-Buy-Entscheidung gehen muss.

Wenn beispielsweise eine Schlüsselperson für mehrere Wochen ausfällt, bleibt die Firewall trotzdem in Betrieb. Änderungen müssen weiterhin geprüft, Störungen bearbeitet und Sicherheitsereignisse bewertet werden.

Eine zeitlich begrenzte externe Unterstützung kann dann eine organisatorische Lücke schliessen, ohne dass die gesamte IT-Struktur verändert werden muss.

Auch bei einem Notfall entscheidet die Vorbereitung

Der Wert eines geregelten Firewall-Betriebs zeigt sich besonders dann, wenn etwas nicht funktioniert.

Eine Netzwerkstörung kann unterschiedliche Ursachen haben. Eine neue Regel kann einen Dienst beeinträchtigen. Ein Update kann unerwartete Auswirkungen haben. Ein Sicherheitsereignis kann eine sofortige Reaktion erfordern.

In solchen Situationen ist nicht nur technisches Fachwissen gefragt. Entscheidend ist auch, ob klar ist, wer reagiert, welche Informationen verfügbar sind und wie eskaliert wird.

NetWyl sieht deshalb definierte Eskalationspfade und klare Kontaktzeiten als Bestandteil des laufenden Betriebs vor. Im Notfall soll das Supportteam unmittelbar analysieren und gezielt reagieren können.

Auch die Übergabe einer bestehenden Umgebung soll strukturiert erfolgen: Review, Übergabe, Testbetrieb und anschliessende Betreuung sollen laut NetWyl ohne Unterbrüche ablaufen.

Das ist ein eher unspektakulärer Teil der IT-Sicherheit - und gerade deshalb leicht zu unterschätzen.

Dokumentation wird zum Sicherheitsfaktor

Eine weitere häufig unterschätzte Aufgabe ist die Dokumentation.

Wer eine Firewall über Jahre betreibt, sammelt nicht nur Regeln, sondern auch Entscheidungen.

- Warum wurde ein bestimmter Zugriff eingerichtet?
- Welche Anwendung benötigt ihn?
- Wer ist verantwortlich?

- Wann wurde die Regel zuletzt überprüft?

Ohne nachvollziehbare Dokumentation hängt dieses Wissen schnell an einzelnen Personen.
Fällt eine Schlüsselperson aus, kann das zum Problem werden.

NetWyl verbindet den laufenden Betrieb deshalb mit dokumentierten Änderungen und nachvollziehbarer Kommunikation. Regeländerungen, Optimierungen und Support sollen nicht nur technisch umgesetzt, sondern auch verständlich dokumentiert werden.

Für Unternehmen ist das mehr als administrative Ordnung. Dokumentation reduziert Abhängigkeiten und schafft eine Grundlage für spätere Reviews, Audits und Fehlersuchen.

Infrastruktur muss sich verändern dürfen

Eine moderne IT-Infrastruktur ist nicht statisch.

Unternehmen migrieren Anwendungen in die Cloud, eröffnen neue Standorte, verändern Arbeitsmodelle oder führen neue digitale Dienste ein. Jede dieser Veränderungen kann Auswirkungen auf Netzwerkarchitektur und Firewall-Regeln haben.

Deshalb kann es sinnvoll sein, Infrastruktur-Sicherheit nicht getrennt von der Weiterentwicklung der IT zu betrachten.

Wenn ein neues System eingeführt wird, sollte frühzeitig geklärt werden, welche Netzwerkzugriffe benötigt werden. Wenn bestehende Anwendungen abgelöst werden, sollten nicht mehr benötigte Regeln verschwinden. Und wenn sich die Architektur verändert, muss auch die Sicherheitsstrategie mitwachsen.

Genau hier liegt die Verbindung zwischen Firewall-Betrieb und allgemeiner IT-Security: Die Firewall ist kein isoliertes Gerät, sondern Teil einer sich verändernden Infrastruktur.

Vom Quick-Check bis zum laufenden Betrieb

Für Unternehmen, die ihre aktuelle Situation nicht vollständig einschätzen können, kann ein strukturierter Blick von aussen ein sinnvoller Ausgangspunkt sein.

NetWyl bietet dafür einen Quick-Check der bestehenden Firewall- und Netzwerksituation an. Darauf können eine Optimierung des Regelwerks oder eine vollständige Betriebsübernahme folgen. Die beschriebenen Leistungen reichen von Updates und Monitoring bis zu Log-Analysen, Störungsbehebung und Reporting.

Ein solcher Ansatz muss nicht zwingend mit einem kompletten Systemwechsel verbunden sein.

Im Gegenteil: Die bestehende Infrastruktur kann zunächst überprüft werden. Anschliessend lässt sich feststellen, welche Regeln sinnvoll sind, wo Dokumentation fehlt und welche Aufgaben intern oder extern übernommen werden sollten.

Das kann insbesondere für Unternehmen interessant sein, die ihre vorhandene Technologie weiter nutzen möchten, aber beim laufenden Betrieb an Kapazitätsgrenzen stossen.

Die wichtigste Firewall-Aufgabe findet nicht bei der Installation statt

Eine Firewall kann technisch leistungsfähig sein und trotzdem zum Risiko werden, wenn ihr Betrieb vernachlässigt wird.

Umgekehrt muss ein Unternehmen nicht zwangsläufig seine gesamte Infrastruktur erneuern, um die Situation zu verbessern. Oft beginnt die Verbesserung bei weniger spektakulären Massnahmen: Regeln überprüfen, Zuständigkeiten

klären, Updates konsequent durchführen, Logs auswerten, Änderungen dokumentieren und einen verlässlichen Prozess für Störungen definieren.

Für NetWyl ist deshalb der laufende Firewall-Betrieb ein Bestandteil eines umfassenderen Security-Betriebs. Die technische Infrastruktur soll nicht einfach funktionieren, sondern dauerhaft gepflegt, überwacht und weiterentwickelt werden.

Die zentrale Frage für Unternehmen lautet damit nicht nur: Welche Firewall haben wir?
Sondern auch: Wer sorgt dafür, dass sie morgen noch sicher, nachvollziehbar und passend zu unserer Infrastruktur betrieben wird?

Hier erfahren Sie mehr über das Team der Netwyl Informatik GmbH: <https://www.netwyl-informatik.ch/ueber-uns/>

NetWyl Informatik GmbH

Täschmattstrasse 19
6015 Luzern

PiotrKusak von Wyl

+41 41 520 07 40

piotr.kusak@netwyl-informatik.ch

www.netwyl-informatik.ch

Portrait

Die NetWyl Informatik GmbH mit Sitz in Luzern ist ein spezialisierter Schweizer IT-Dienstleister für Cybersecurity und Netzwerklösungen. Das Unternehmen unterstützt KMU sowie größere Organisationen bei der Absicherung ihrer IT-Infrastrukturen durch maßgeschneiderte Sicherheitskonzepte, Managed Security Services, E-Mail-Security, Cloud-Lösungen und Sicherheitsanalysen. NetWyl kombiniert langjährige IT-Security-Expertise mit persönlicher Beratung und verfolgt das Ziel, Unternehmen zuverlässig vor Cyberrisiken zu schützen und einen sicheren, stabilen IT-Betrieb zu gewährleisten.

News-ID: 1327324 • Views: 94 (Stand: 30.10.2026)

Link zur Pressemitteilung:

<https://www.openpr.de/news/1327324/Firewall-Sicherheit-beginnt-mit-dem-laufenden-Betrieb.html>