

lista office **LO**

# Ein Penetration Test bringt Klarheit

## Ein Interview mit Thomas Friederich, dem IT-Leiter von Lista Office LO

**Welchen Herausforderungen stehen Sie als IT-Leiter gegenüber?** Die IT-Landschaft hat sich bei der Lista Office in den letzten Jahren stark verändert. Die IT-Infrastruktur ist nicht mehr bei uns im Hause und wir setzen mittlerweile konsequent Microsoft 365 ein. Zudem sind viele Mitarbeitende zunehmend mobil unterwegs und müssen von überall Zugriff auf die notwendigen Daten haben. Weiter müssen wir die Mitarbeitenden zunehmend auf die Gefahren im IT-Umfeld sensibilisieren, was nicht immer so einfach ist. Weiter kommt hinzu, dass die IT-Kosten nicht ansteigen sollten. Das Ziel ist also eine möglichst optimierte, flexible und sicherheitsbewusste IT-Infrastruktur zu einem vernünftigen Preis.

**Wie gehen Sie mit dem Thema IT- und Cyber- Security um?** Wir haben die IT-Sicherheit immer im Fokus, früher vor allem in Bezug auf das Eindringen von aussen und den Virenschutz. Auch in die E-Mail-Sicherheit haben wir früher, als wir die IT-Infrastruktur noch selbst betrieben hatten, einiges investiert. Heute mit dem Wandel unserer IT durch die Nutzung von Cloud-Diensten und die Auslagerung der Server, Netzwerkinfrastruktur und dem Clientmanagement ist vieles anders geworden.

In den letzten Monaten häufen sich die Nachrichten bezüglich Cyber Attacken, was uns dazu bewogen hat, das Thema der IT-Security genauer anzuschauen. Wir gingen davon aus, dass wir grundsätzlich eine ziemlich sichere IT-Landschaft

## Herausforderung und Lösung:

Liste Office LO schafft Bürowelten, die Tag für Tag mit viel Liebe für das Detail Menschen begeistern. Die rund 350 Mitarbeiter engagieren sich für die Kundenwünsche, um die bestmögliche Qualität in jeglicher Hinsicht zu liefern. Ein Unternehmen in dieser Grösse steht im Fokus von möglichen Cyber Angriffen. Änderungen in der IT-Landschaft, Auslagerungen in externe Rechenzentern und mobiles Arbeiten von Zuhause aus oder unterwegs schaffen potentielle Gefahren für das Unternehmen. Aus diesem Grund wurde von Selution ein unabhängiger und neutraler Penetration Test durchgeführt. In unserem Interview mit Herr **Thomas Friederich**, dem IT-Leiter von Lista Office LO, gehen wir genauer auf das Projekt ein.

haben. Wir wollten aber sehen, ob wir irgendwo «blinde Flecken» haben oder anders gesagt: Haben wir irgendwo «Türen» offen, welche wir aber als geschlossen betrachten und die es tatsächlich dann gar nicht sind? Genau das wollten wir herausfinden. Weiter sind IT-Awareness Schulungen für die Mitarbeitenden geplant, aus meiner Sicht ist das grösste Risiko immer noch der einzelne PC-Anwender.

**Beunruhigen Sie die täglichen Meldungen von Cyber-Angriffen auf verschiedene Unternehmen?** Die Häufung der Meldungen von Angriffen und Erpressungen bei Schweizer Firmen finde ich schon besorgniserregend. Es zeigt, dass nicht mehr nur Gross- oder Hightech-Firmen die Ziele sind, sondern durchaus auch mittelständische Unternehmen, wie wir eines sind. Was ich persönlich besonders schlimm finde ist, dass in keinem Fall, von dem ich gehört habe, von aussen gehackt wurde, sondern mit Hilfe von verschickten Trojanern ein Zugang geschaffen wurde. Das schwächste Glied in der Kette ist leider der Mensch.

**Was waren für Sie die wichtigsten Erkenntnisse aus dem durchgeführten Test?** Die Tests haben gezeigt, dass wir von aussen gut geschützt sind. Aber wenn ein Angreifer mal im Netz drin ist, stehen ihm viele Türen offen. Diese sind nun geschlossen. Die Auflistung der Resultate von Selution mit der entsprechenden Priorisierung hat uns also geholfen, die notwendigen Sofortmassnahmen umzusetzen. Bei Rückfragen standen uns die Spezialisten von Selution zur Verfügung.

**Ziehen Sie es in Betracht, die Überprüfung der Infrastruktur regelmässig durchzuführen?** Ja, das ziehe ich tatsächlich in Betracht. Es war mir bewusst, dass wir beim ersten Check mal eine Grundübersicht haben würden (eben ein Health-Check) und dass wir daraus Massnahmen ableiten werden. Wenn man schaut, wie schnell der Wandel in der IT ist, wo mit jedem Patch, jedem neuen IoT-Gerät neue Sicherheitslücken geschaffen werden können, wird klar, dass eine regelmässige Überprüfung notwendig sein wird.

**Wieso haben Sie sich für einen unabhängigen Partner gerade für Selution entschieden, um Ihre Infrastruktur zu testen?** Wir haben uns überlegt, in welcher Form wir einen solchen Test durchführen möchten und haben dann einige mögliche Anbieter kontaktiert. Diese Anbieter haben uns dann ihre Lösungsvorschläge präsentiert, wobei uns dann der Vorschlag von Selution am meisten überzeugt hat. Dies nicht nur wegen der Vorgehensweise, sondern auch wegen des Preis-Leistungs-Verhältnisses.

**Herr Friederich, haben Sie abschliessende Worte für uns?** Ich denke, als IT-Verantwortlicher muss man sich den Gefahren bezüglich Security und Cyberangriffen bewusst sein. Da bin ich auch sehr froh, dass ich in meinem IT-Team mit Daniel Weibel einen erfahrenen Mitarbeiter habe, welcher sich um das Thema IT-Security kümmert. Es ist aber auch so, dass mit der zunehmenden Vernetzung und mittlerweile vielen Cloud-Services, welche wir nutzen, teilweise der Aspekt der IT-Security auch etwas verloren geht. Oftmals entsteht auch ein Konflikt zwischen den Fachabteilungen, welche in erster Linie den Nutzen von neuen Software-Lösungen sehen und der IT, welche dann teilweise gewisse Ideen aus Security-Gründen verbieten oder blockieren muss. Das kommt verständlicherweise nicht überall gut an. Ich denke, es braucht ein gutes Miteinander zwischen den Fachabteilungen und der IT und entsprechende Konzepte, falls ein Vorfall eintreten sollte. Dann ist es auch sehr hilfreich, wenn man auf externe Partner zurückgreifen kann, welche in diesen Bereichen einfach mehr Erfahrung haben als wir. Wir (also unsere IT) sehen vor allem unsere eigenen Bereiche (also die eigene IT-Infrastruktur) und da sind wir auch auf die Unterstützung von Partnern angewiesen. Am Schluss liegt es aber bei uns, zu entscheiden, wann wir welche Massnahmen treffen müssen. Diese Entscheidung kann einem niemand abnehmen.



**Thomas Friederich**

IT-Leiter bei Lista Office LO | [www.lista-office.com](http://www.lista-office.com)

Thomas Friederich ist für die gesamte Informatik der Lista Office verantwortlich und betreut mit dem Team die gesamte IT-Infrastruktur im Unternehmen. Aufgrund stetig steigenden Druckes durch die Umwelt im Bereich Security und sich verändernden Anforderungen im Unternehmen hat er sich dazu entschieden, einen Audit mit Selution durchzuführen.

# Machen auch Sie den Test – bevor es zu spät ist.

## Testen Sie Ihre IT-Landschaft

Durch einen gezielten Hackerangriff wird innerhalb des Penetration Test ersichtlich, welche Schwachstellen im Netzwerk vorhanden sind. Dank einer detaillierten Identifizierung und Verifizierung wird Ihrem System dadurch niemals geschadet.

## Identifizieren Sie Ihre Sicherheitslücken

Potentielle Angriffsflächen und Risiken werden auf einen Blick ersichtlich. Im Kontext zu Ihren Geschäftsprozessen können diese bewertet und eingestuft werden.

## Priorisieren, planen und setzen Sie Ihre Massnahmen um

Eine Adressatengerechte und massgeschneiderte Auswertung hilft Ihnen die Sicherheitslücken besser zu verstehen. Dank unseren Erkenntnissen und den Empfehlungen können Sie die Massnahmen direkt umsetzen – selbstverständliche unterstützen wir Sie auch in diesem komplexen Prozess.

**Testen Sie Ihre IT-Infrastruktur, bevor es Hacker tun. Wir helfen Ihnen dabei.**



**Selution AG**  
www.selution.ch  
info@selution.ch  
+41 58 531 00 00

## Über Selution

Selution ist ein Cyber Security Experte mit verschiedenen Ausprägungen. Unter anderem sind wir auf Ehtical Hacking mit Fokus auf Penetration Testing spezialisiert. Wir helfen dabei die Unternehmenssicherheit zu erhöhen, damit auch Sie wieder ruhiger schlafen können.

Unsere langjährige Erfahrung im Cyber Security Bereich schützt nicht nur Sie, sondern auch Ihr Umfeld wie Partner, Lieferanten und Familie. Da uns Ihre Sicherheit wichtig ist, engagieren wir uns aktiv in Cyber Security Organisationen, z.B. bei Swiss Cyber Experts, Information Security Society Switzerland und weiteren Vereinigungen.

mehr auf [selution.ch/cyber-security](https://www.selution.ch/cyber-security)