Die Vorarlberger IT-Security Experts informieren

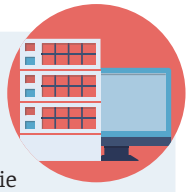
Die Kernaufgabe der IT-Security Experts Vorarlberg ist die Verbesserung der Informations- und IT-Sicherheit von Vorarlberger Unternehmen. In den folgenden acht Fachbeiträgen informieren sie exklusiv über Gefahren und Lösungsansätze im Informations- und IT-Bereich.

Internet of Things „IoT“

Alle erdenklichen Geräte wie Kaffeemaschinen, Rollos und sogar die Heizung können über standardisierte Protokolle miteinander kommunizieren und ferngesteuert werden. Wenn Sie etwas früher nach Hause kommen, drehen Sie die Heizung per Smartphone etwas eher hoch oder schalten die Kaffeemaschine ein. Doch dieser Luxus birgt auch große Gefahren in sich. So gibt es Suchmaschinen, die das Aufspüren von Geräten wie Überwachungskameras oder Lichtsteuerungen im Internet kinderleicht machen. Kriminelle können dann die Geräte selber angreifen oder sogar in Ihr Netzwerk eindringen und möglicherweise Daten stehlen. Daher empfiehlt die IT-Security Experts, alle Geräte immer auf dem aktuellen Softwarestand zu halten, die Passwörter möglichst komplex zu wählen und keinesfalls dieselben mehrfach zu verwenden. Sinnvoll ist es auch, diese Geräte in einem separatem Netzwerk anzusiedeln.

Georg Dörn
its-doern e.U.
www.its-doern.at

Backup Strategien



Backups sind ein heikles Thema. Backups sind wie Verträge: Man braucht sie dringend, man hofft, sie niemals zu brauchen und obendrein kosten sie ein Vermögen. Ich spreche hier nicht über ein Image eines virtualisierten Servers, sondern über das Backup von SAN oder NAS. Diese sind so groß, dass man weitere NAS für komplette Backups benötigt. Wie macht man das jetzt am besten? Die Sicherungsarten Differenziell und Inkrementell helfen dabei, Speicherplatz zu sparen. Speicherplatz sparen, spart Geld. Bei einem teilweisen Backup muss gewisse Zeit für das Restaurieren der Daten einkalkuliert werden. Beim kompletten Backup hat man sofort Zugang zu den Daten. Probleme gibt es, wenn ein Backup wegen eines Ransom-Virus benötigt wird. Wie alt ist das Backup? Ist das Virus dort ebenfalls schon drauf? Wie weit kann man auf ein Backup zurückgreifen, dass der Geschäftsschaden vertretbar bleibt? Das sind alles existenzrelevante Fragen für Ihr Unternehmen. Sprechen Sie unbedingt mit Ihrem Systembetreuer über dieses Thema.

Roland Schaffer
schaffer-se
www.schaffer-se.at

Wer schützt Ihre IT-Systeme?

Nie waren wir mehr von IT abhängig. Doch dies bedeutet auch ein hohes Risiko, wenn es einmal Probleme gibt. Wenn wir auf Daten, Dateien oder E-Mails nicht zugreifen können, kann sich dies direkt auf die Ertragssituation auswirken. Wie gut sind Sie vorbereitet? Heutzutage ist es schwieriger denn je, IT-Systeme vor Bedrohungen aus dem Internet zu schützen. Im Zeitalter hochentwickelter Systeme und hohem IT-Bewusstseins ist die Datensicherheit für jedes Unternehmen, das um die möglichen Auswirkungen einer Sicherheitslücke Bescheid weiß, ein wichtiges Anliegen. Eine Antwort hierauf sind Remote Management Lösungen. Ihre IT-Systeme werden dabei überwacht, geschützt und analysiert, damit Ihr Geschäftsalltag problemlos weiterlaufen kann.

Andreas Wieser
IDEEFIX System- und Softwareentwicklung
www.ideefix.eu

Darknet – die dunkle Seite des Internet

Darknet wurde ursprünglich geschaffen, um amerikanischen Geheimdienst-Mitarbeitern Sicherheit und Anonymität zu gewährleisten. Heute ist es ein Umschlagplatz für Kriminelle. Waffen, Drogen, gefälschte Dokumente und User-Daten werden hier ebenso gehandelt wie Anleitungen zum Kreditkarten-Missbrauch. Finanztransaktionen werden mit Bitcoins durchgeführt. Darknet benötigt spezielle Browser und ist über herkömmliche Suchmaschinen nicht zu finden. Die dunkle Seite des Internet bestätigt einmal mehr die Wichtigkeit, Daten und Identitäten zu schützen. Besonders KMU stehen im Fokus der Online-Kriminalität. Dagegen helfen unternehmensweite Sicherheitsmaßnahmen, die von umfassenden Schutzvorkehrungen bis zur Sicherheitssensibilisierung der Mitarbeiter reichen. Sicherheitsbewusste Unternehmer schaffen sich so Wettbewerbsvorteile: Auf Basis einer detaillierten Sicherheitsanalyse wird ein Statusbericht mit Empfehlungen dringender Sicherheitsmaßnahmen angefertigt. Es folgt ein professionelles Sicherheitskonzept, das strategische Entscheidungen im Hinblick auf personelle und organisatorische, technische und bauliche Einrichtungen und Sicherheitsmaßnahmen ermöglicht. Dazu gehören Sicherheitsrichtlinien, Notfallpläne und Schulungen, damit sich im Ernstfall die Mitarbeiter richtig verhalten.

Wolfgang Hödl
PROfIT Management Hödl KG
www.profit-management.at

Kryptowährungen

Haben Kryptowährungen eine Zukunft oder fördern sie nur den kriminellen Onlinehandel?
Eine Kryptowährung ist Geld in digitaler Form, welches auf einer Software beruht und in erster Linie von sogenannten „Minern" erzeugt wird. Das Besondere daran ist die dezentrale Steuerung, also ohne staatliche Eingriffe oder Finanzinstitutionen. Der Bitcoin ist der Vater und bekanntester Vertreter der Kryptowährungen. Die enorme Marktkapitalisierung (aktuell ca. sechs Milliarden Euro) des Bitcoins führte zur Entstehung einer Reihe alternativer virtueller Währungen wie beispielsweise dem Faircoin oder Litecoin. Der Bitcoin und sein Einsatz werden jedoch kontrovers diskutiert. Die systembedingte Anonymität kann einerseits im Sinne des Datenschutzes und der Privatsphäre als Vorteil gesehen werden, andererseits kann diese Anonymität zu Missbrauch führen, da betrügerische Geldflüsse nicht nachvollzogen werden können. Die aktuelle Vielfalt an Erpresser-Viren verlangen bspw. eine Bezahlung mit Bitcoins. Skeptiker erwähnen zudem das hohe Spekulationspotenzial. Täglich werden Bitcoins im Wert von über zwei Millionen Euro an den verschiedenen Onlinebörsen gehandelt. Als Spekulationsobjekt ist es vergleichbar mit hoch riskanten Finanzprodukten. Dies gilt besonders für die vielen neuen Kryptowährungen. Der Name Bitcoin wird wohl auch in Zukunft eher negativ behaftet sein, jedoch ist zu erkennen, dass viele regionale und nationale Währungsprojekte die Bitcoin Software verwenden.

Christian König
LINUXIT König OG
www.linuxit.at

Warten auf Totalausfall

Kleine und mittelständische Unternehmen verfolgen oft eine Strategie der „Feuerwehr-Reparatur". Funktioniert etwas nicht mehr, bzw. ist etwas kaputt, wird es durch die IT (intern oder extern) repariert bzw. wiederhergestellt. Gerade in Zeiten von Cryptolocker, Blackouts, falschen Supportanrufen wird es immer wichtiger, die Systeme zu überwachen und zu patchen (Sicherheitsupdates einspielen). Auch die Schulung der Anwender im Bereich IT-Security sollte einen großen Stellenwert einnehmen. Mittels Erpressungstrojanern oder falschen Supportanrufen werden Daten gestohlen oder verschlüsselt. Um die Daten wieder zu entschlüsseln, werden teils hohe Summen verlangt (z.B. 1,3 Bitcoins – ca. 500,- Euro). Die Probleme werden trotz Zahlung nicht vollständig behoben. Ausfälle und Datenverlust sind die Folge. Im Falle von Ransomware wie Locky, Petya usw. sind Backups die letzten Verteidigungslinien.
Tipps: E-Mail-Anhänge (derzeit besonders Word) NUR von bekannten Absendern öffnen (Makros deaktivieren); System aktuell halten (Microsoft Updates); Mehrstufiger Virenschutz (z.B. Firewall mit Virenschutz und lokaler Virenscanner); Keiner fremden Person Zugriff auf Ihr System gewähren; Regelmäßige Datensicherung (3-2-1 Methode).

Horst Kasper
Rescue EDV e.U.
www.rescue.at

Die Cloud

Cloud-Computing und Cloud-Speicher. Segen oder Fluch für Datensicherheit und Betriebsgeheimnisse?
Im heutigen Zeitalter der Cloud werden sämtliche Daten und Programme von externen Servern zur Verfügung gestellt, d.h. Verwaltungstools wie CRM (customer relationship management) Software werden im Web abgebildet. Den Vorteil, den Sie dabei erlangen, ist, dass Sie keine großen Backups von Ihrem Server erstellen müssen. Aber vertrauen Sie dem Drittanbieter, der Ihre Daten hat? Die Problematik bei solchen Cloud-Lösungen ist die Weitergabe sensibler Daten in die falschen Hände, denn dadurch kann ein großer finanzieller Schaden entstehen. Doch die Bequemlichkeit des Menschen arbeitet gegen den Verstand, Dokumente und Programme sicher im betriebsinternen Netzwerk zu schützen. Wir wollen immer und überall von jedem Gerät, Smartphone oder Notebook, auf all unsere Daten und Programme zugreifen können. Dies führt dazu, dass immer mehr im Internet erscheint, das so nicht geplant war. Die Cloud sollte noch mit Vorsicht genossen werden, das Backup auf den eigenen Speichermedien ist meiner Meinung nach immer noch das Beste.

Andreas Fritz
FritzComputing
www.fritzcomputing.at

Sichere Konfiguration Ihres WLAN

Falls Sie Kunde von UPC sind, haben Sie wohl schon eine Nachricht dazu erhalten. Durch eine Sicherheitslücke sind die voreingestellten WLAN Kennwörter nicht sicher. Diese müssen deshalb unbedingt geändert werden. Entstanden ist das Problem, da der verwendete Key aus der, an sich geheimen, Seriennummer des Routers errechnet wurde. Da jedoch auch der Netzwerkname selbst (die SSID) sich daraus ableitet, konnte von einem Sicherheitsexperten ein Zusammenhang errechnet werden. Mit zwei einfachen Schritten kann nun mit einem Web-Tool das Kennwort aus der SSID errechnet werden. Damit kann also jeder in das Netz eindringen und dann auch den Verkehr mithören. Da meist auch das Administrator-Kennwort des Routers selbst nicht sicher ist, kann der Angreifer auch jegliche Einstellungen ändern. Neben dem Abgriff von Daten könnte auch ein Schaden durch Nutzung des Telefonanschlusses entstehen. Studien zufolge sieht es bei anderen Providern keineswegs wesentlich besser aus. Die Standardeinstellungen sind oft nicht sehr sicher. Wir empfehlen deshalb jedenfalls bei Inbetriebnahme eines Funknetzwerkes, eigene Einstellungen zu setzen. Die SSID, der Netzwerkname kann durchaus eine sprechende Bezeichnung sein wie BestesNetzDerWelt, sollte aber, wenn möglich, nicht unbedingt mit Ihnen im direkten Zusammenhang stehen, falls es ein Hacker auf Sie abgesehen hat. Das Kennwort sollte aus Groß- und Kleinbuchstaben und Zahlen oder Sonderzeichen bestehen und eine Länge von etwa zehn Zeichen umfassen.

Manuel Glojek
grasgruen.it
www.grasgruen.it