Wie Unternehmer tatsächlich sicher sein können!

Für Unternehmer gehören Ransomware-Attacken zu den meistgefürchteten Angriffen durch Hacker und Datendiebe. Unser Privacy -und Datenschutz-Experte schafft Klarheit in den wichtigsten Aspekten.

KONVERTO: Martin, was genau ist eigentlich Ransomware und wie läuft eine solche Attacke ab?

Martin Galler: Der Name Ransomware kommt aus dem Englischen und umschreibt eine Lösegeldforderung. Datendiebe kontaktieren Mitarbeiter eines Unternehmens meist per E-Mail und fordern sie auf einen Link zu klicken, oder Dateien herunterzuladen. Dadurch dringen sie in das Unternehmensnetz ein und verschlüsseln wichtige oder sensible Daten. Um diese wieder zugänglich zu machen, verlangen die Hacker hohe Summen an Lösegeld. Das Geschäftsmodell funktioniert, weil die Lösegeldforderungen in den meisten Fällen geringer als die Wiederherstellungskosten sind.

KONVERTO: Wie bedeutend sind Ransomware-Attacken für Unternehmer wirklich?

Martin Galler: Bereits seit 2013 sind Ransomware-Attacken ein Massenphänomen. Erschreckend ist jedoch vor Allem die technische Entwicklung der letzten Jahre. Man kann kaum mehr von vereinzelten Angriffen sprechen, es handelt sich um organisierte Kriminalität. Hacker haben ihre Strategie soweit verbessert, dass sie Unternehmen bereits vor dem Angriff ausspähen und beobachten, sodass sie Schwachstellen ermitteln und den Erstbefall verbessern können. Immer häufiger werden sensible Daten exportiert und Backups gelöscht. Zudem hat die Möglichkeit, Versicherung gegen Cyberangriffe abzuschließen, die Lösegeldforderungen beachtlich erhöht, weil es wahrscheinlicher ist, dass versicherte Unternehmen zahlen.

Eine aktuelle bitkom-Studie zeigt auf, wie weit verbreitet Ransomware-Attacken eigentlich sind. Etwa 88% der befragten Unternehmen waren innerhalb der letzten 12 Monaten von Diebstahl, Industriespionage oder Sabotage betroffen. Und der Trend scheint zu steigen, denn erst vor zwei Jahren lag diese Zahl noch bei 75%. Diese Zunahme betrifft jede Branche und Unternehmensgröße, kein Unternehmen kann sich in Sicherheit wiegen.

KONVERTO: Wie können sich Unternehmen gegen solche Angriffe effizient schützen?

Martin Galler: Um einen Angriff von vorneherein abzuwehren, gilt es zwei entscheidende Maßnahmen umzusetzen. Auf technischer Ebene müssen Systeme und Softwares immer aktualisiert sowie eine Firewall, Antivirus- und Filterprogramme eingesetzt werden. Sie bilden eine erste Barriere gegen Schadsoftware. Sollte eine infizierte E-Mail trotzdem durch diese Sicherheitsbarrieren gelangen ist wird Sensibilisierung zum Stichwort. Wenn Mitarbeiter laufend informiert werden und die Tricks der Angreifer kennen, ist ein erfolgreicher Angriff um einiges unwahrscheinlicher.

KONVERTO: Welche konkreten Tipps kannst du Unternehmern und Mitarbeitern geben?

Martin Galler: Generell gilt es, unerwartete oder auffällige E-Mails vor jeglicher Aktion zu prüfen, da die meisten Ransom-E-Mails gemeinsame Aspekte aufweisen. Oft enthalten sie Rechtschreib- oder Grammatikfehler, sind in einem unstimmigen Ton verfasst oder kommen von vorgetäuschten Absendern. Meist versuchen Absender den Empfänger unter Zeitdruck zu stellen, Angst einzuflößen oder einzuschüchtern. Weist eine E-Mail einen dieser Aspekte auf, sollte sie unbedingt signalisiert werden, um eine Infektion zu vermeiden.

Come gli imprenditori possono davvero essere al sicuro!

Gli attacchi ransomware sono tra gli attacchi di hacker e ladri di dati più temuti dagli imprenditori. Il nostro esperto di privacy e protezione dei dati fornisce chiarezza sugli aspetti più importanti.

KONVERTO: Martin, cos'è esattamente il ransomware e come funziona un attacco di questo tipo?

Martin Galler: Il nome ransomware viene dall'inglese e indica una richiesta di riscatto. I ladri di dati di solito contattano i dipendenti di un'azienda via e-mail e chiedono loro di cliccare su un link o di scaricare dei file. Così facendo, si infiltrano nella rete aziendale e criptano i dati importanti o sensibili. Per rendere questi documenti nuovamente accessibili, gli hacker chiedono grandi somme di denaro come riscatto. Il modello di business funziona perché le richieste di riscatto sono generalmente inferiori ai costi di recupero.

KONVERTO: Quanto sono realmente significativi gli attacchi ransomware per gli imprenditori?

Martin Galler: Gli attacchi ransomware sono un fenomeno di massa dal 2013. Tuttavia, lo sviluppo tecnico degli ultimi anni è particolarmente spaventoso. Non si può più parlare di attacchi isolati, si tratta ormai di criminalità organizzata. Gli hacker hanno migliorato la loro strategia a tal punto da spiare e osservare le aziende ancora prima di attaccare, in modo da poter identificare i punti deboli e migliorare l'attacco iniziale. Sempre più spesso esportano i dati sensibili e cancellano i backup. Inoltre, la possibilità di stipulare un'assicurazione contro gli attacchi informatici ha aumentato notevolmente le richieste di riscatto, perché le aziende assicurate sono più propense a pagare.

Un recente studio di Bitkom mostra quanto siano diffusi gli attacchi ransomware. Circa l'88% delle aziende intervistate sono state colpite da furto, spionaggio industriale o sabotaggio negli ultimi 12 mesi. E la tendenza sembra essere in aumento, visto che solo due anni fa questa cifra era ancora al 75%. Questo incremento colpisce ogni industria e dimensione aziendale, nessuna azienda può considerarsi al sicuro.

KONVERTO: Come possono le aziende proteggersi efficacemente da questi attacchi?

Martin Galler: Per prevenire un attacco fin dall'inizio, è necessario attuare due misure decisive. A livello tecnico, i sistemi e i software devono essere sempre aggiornati e occorre utilizzare un firewall, un antivirus e programmi di filtraggio. Questi strumenti formano una prima barriera contro il malware. Se un'e-mail infetta riesce a superare queste barriere di sicurezza tecniche, la parola chiave è "sensibilizzazione". Informando costantemente i dipendenti e aggiornandoli sui trucchi degli attaccanti, un attacco di successo è molto meno probabile.

KONVERTO: Quali consigli specifici puoi dare agli imprenditori e ai dipendenti?

Martin Galler: In generale, è importante controllare le email inaspettate o sospette prima di intraprendere qualsiasi azione, poiché la maggior parte delle email di riscatto hanno aspetti comuni. Spesso contengono errori ortografici o grammaticali, sono scritti con un tono incoerente o provengono da mittenti falsi. Nella maggior parte dei casi, i mittenti cercano di mettere il destinatario sotto pressione, incutere paura o intimidirlo. Se un'e-mail ha uno di questi aspetti, deve essere assolutamente segnalata per evitare un attacco.