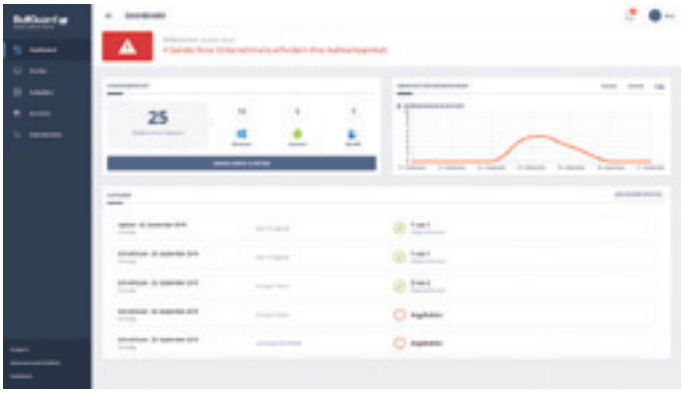
CYBERANGRIFFE:

IT-Sicherheit im **Bauhandwerk**

Jeder zweite Cyberangriff trifft ein kleines Unternehmen. Zu diesem Ergebnis kam der aktuelle Verizon 2019 Data Breach Investigations Report. Für Hacker sind diese Betriebe leichte Beute, weil sie weniger Know-how, Zeit und Budget für IT-Sicherheit zur Verfügung haben als große Konzerne | VON STEFAN WEHRHAHN



Mit einer Security-Lösung eigens für kleine Unternehmen wird IT-Sicherheit für Handwerksbetriebe zum Kinderspiel.

Hürden bei der Cyber-Sicherheit: Viele Handwerksbetriebe wägen sich zu Unrecht in Sicherheit, weil sie glauben, kein attraktives Ziel für Hacker zu sein. Oft mangelt es kleinen Betrieben aber an Zeit und Budget, um sich umfassend vor Cyber-Angriffen zu schützen. Und meist gibt es keinen Mitarbeiter, der dediziert für das Thema IT-Sicherheit zuständig ist und entsprechendes Know-how einbringen kann. Gleichzeitig kämpfen Handwerker mit Security-Lösungen, die nicht auf ihre Situation zugeschnitten sind. Entweder nutzen die zehn bis 15 Mitarbeiter einzelne Consumer-Lösungen. Oder der Betrieb setzt auf komplexe Enterprise-Software, die zwar um Funktionen reduziert wurde, aber trotzdem schwierig zu handhaben und gleichzeitig teuer ist.

Die Corona-Krise verschärfte die Lage: Auch im Baugewerbe wurden Arbeitsplätze ins Home Office verlagert, um von dort Anfragen, Aufträge und Abrechnungen zu koordinieren. Die dafür notwendige IT-Infrastruktur wurde meist kurzfristig und ohne entsprechende Überprüfung aufgesetzt. Hacker kennen die Situation in den Betrieben und machen sich diese zunutze: Über Phishing-Mails oder gefälschte Websites gelangen sie ins Unternehmensnetzwerk, um dort Kontodaten, Kundeninformationen oder Passwörter abzugreifen. Findige Betrüger geben auch vor, bei der Beantragung von Corona-Hilfen zu unterstützen, zweigen die Gelder dann aber für sich selbst ab.

Maßnahmen für mehr IT-Sicherheit im Baugewerbe

IT-Sicherheit in kleinen Betrieben umzusetzen, ist mit besonderen Herausforderungen verbunden. Dabei ist es hilfreich, zwei Partner an der Seite zu haben: einen regionalen IT-Dienstleister, der bei Bedarf das komplette Management der IT-Infrastruktur übernehmen kann, und eine Security-Lösung, die speziell auf die Bedürfnisse kleiner Betriebe zugeschnitten ist, wie etwa BullGuard Small Office Security. Sie liefert professionelle Endpoint-Security, um vor Datendiebstahl, Malware und anderen Cyberangriffen zu schützen, bringt aber nur Funktionen mit, die im Unternehmen auch wirklich gebraucht werden. Ein übersichtliches Dashboard hilft dabei, die IT-Sicherheit des Betriebs für bis zu 50 Geräte zu verwalten. Die Lösung macht auf Sicherheitsprobleme aufmerksam und schlägt sofort passende Gegenmaßnahmen vor. Sie eignet sich damit insbesondere für Dachdeckerbetriebe, Elektroinstallateure, Malerbetriebe, Sanitär-, Heizungs- und Klima-Betriebe sowie Planungs- und Ingenieurbüros. Zusätzlich schützen sich kleine Betriebe mit den folgenden drei Ratschlägen besser vor Cyberangriffen:

1. Regelmäßig Sicherungskopien erstellen: In regelmäßigen Abständen, zum Beispiel täglich oder wöchentlich, sollten Sicherungskopien sämtlicher Daten erstellt werden. Diese sind vorzugsweise außerhalb des eigenen Netzwerks abzuspeichern. So machen sich Betriebe unabhängig von Hackern, die etwa im Zuge eines Ransomware-Angriffs sämtliche Daten löschen und hohe Lösegeld-Forderungen verlangen, um sie wiederherzustellen.

2. Virenschutz immer aktuell halten: Der eingesetzte Virenschutz sollte immer auf dem aktuellsten Stand sein. So wird sichergestellt, daß die Software die neusten Schadprogramme findet und umfangreich vor Malware schützen kann. Eine entsprechende Antivirus-Software, die speziell für kleine Unternehmen geeignet ist, weist auf notwendige Updates hin und unterstützt bei der schnellen Aktualisierung aller Geräte. So können Betriebe den Aufwand für IT-Sicherheit möglichst kleinhalten, aber gleichzeitig für größtmögliche Sicherheit sorgen.

Stefan Wehrhahn, Country Manager DACH, BullGuard (Alle Bilder: Bullguard)

3. Mitarbeiter für Gefahren sensibilisieren und schulen: Menschliches Versagen ist eine der häufigsten Ursachen für einen Cyberangriff. Unachtsamkeit oder auch Unwissen öffnen Hackern Tür und Tor, sei es durch Klicken auf einen bösartigen Link in einer E-Mail, durch den Besuch von Websites, die schadhaften Code verstecken, oder durch verlorengegangene Geräte. Daher ist es wichtig, daß die Mitarbeiter für diese Gefahren entsprechend sensibilisiert werden. <<

Noch Fragen?
https://www.bullguard.com/de/business.aspx