



SIMPLY
SECURE

ZUVERLÄSSIGER SCHUTZ EGAL, WO.

ZUVERLÄSSIGER SCHUTZ FÜR EINE MOBILE UMGEBUNG

KUNDE

- Ducati Corse
- Land: Italien
- Zu schützende Umgebung:
IT-Systeme an der Rennstrecke

DIE HERAUSFORDERUNG

- Bereitstellung eines proaktiven Schutzes sowohl gegen interne als auch externe Bedrohungen sowie die Wahrung der Integrität von Renndaten

DIE LÖSUNG

- Überdurchschnittliche Erkennungsraten für Schadsoftware und ausgezeichnete Prävention
- Remote-Management
- Einfache Konfigurierbarkeit von Sicherheits-Policies

DIE VORTEILE

- Minimierung unbefugter Zugriffe
- Echtzeitinformationen



Was die IT-Sicherheit angeht, hat Ducati klare Vorstellungen. In erster Linie: die Vertraulichkeit und Integrität der 20 GB an Daten, die an jedem Rennwochenende von den Sensoren der Maschinen erzeugt werden.

Im Jahr 1926 gründete die Familie Ducati zusammen mit einigen lokalen Investoren in Bologna die Società Radio Brevetti, um im großen Stil Bauteile nach den Patenten Adriano Ducatis für den wachsenden Markt der Radioempfänger herzustellen. Das erste Produkt aus dem Hause Ducati, der Manens-Kondensator, ermöglichte der Firma ein schnelles Wachstum und sicherte ihr internationale Anerkennung in der Branche. Im September 1946 verlagerte man mit Einführung des Cucciolo, eines kleinen Hilfsmotors für Fahrräder, der internationale Berühmtheit erlangen sollte, die Produktion. Innerhalb kurzer Zeit wurde aus dem Cucciolo ein echtes kleines Motorrad. Dank des Erfolgs des Cucciolo und seiner Nachfolger konnte sich die Marke Ducati einen festen Platz in der Motorenbranche sichern.

Das Abenteuer MotoGP begann für Ducati im Jahr 2003, mit der Desmodedici und den Fahrern Troy Bayliss und Loris Capirossi. Heute ist Ducati Corse eine Ducati Holding Company mit etwa 200 Angestellten, darunter 60 „Nomaden“, die für 250 Tage im

Jahr außer Haus arbeiten. Ducati Corse fällt also in die Größenordnung eines kleinen- bis mittelständischen Unternehmens. Dass man in der Lage ist, sich sportlich gegen Rennabteilungen anderer Firmen durchzusetzen, die über drei- bis achtmal mehr Personal verfügen, erfüllt das Team mit Stolz, aber verlangt ihm auch eine Menge ab. Hinter den wenigen Minuten des eigentlichen Rennens stehen 30.000 Stunden mit Simulationen, 25.000 Stunden Fahrzeug- und Motorenentwicklung sowie Windkanaltests und zahlreiche andere Aufgaben, die am Ende den Erfolg des Ducati-Teams sichern.

Der Kern der IT von Ducati, welcher bei allen MotoGP-Rennen dabei ist, verbringt 300 Tage im Jahr auf Reisen. Ein vollständiges Rechenzentrum mit Servern, Firewalls, Routern und aller erforderlichen Hardware erlaubt es dem Team hinter den Fahrern, sich ganz auf die Rennparameter zu konzentrieren, auf alle erforderlichen Einstellungen sowie die Analyse der Daten, die während der gesamten vier Tage um das Rennen herum angesammelt werden. Die Systeme, die auf den

„DIE G DATA LÖSUNG HAT SICH AUF EINER MARTERSTRECKE WIE DER MOTOGP ALS SEHR WIRKSAM ERWIESEN.“

Stefano Rendina, IT-Manager, Ducati Corse

Rennstrecken eingesetzt werden, kommen immer nur für kurze Zeit nach Borgo Panigale zurück. In dieser kurzen Zeit werden zum einen Systemupdates durchgeführt, die diejenigen ergänzen, welche die ganze Zeit über aus der Ferne vorgenommen werden. Zum anderen werden während dieser kurzen „Boxenstopps“ auch Neukonfigurationen eingespielt.

Infektionen durch Viren oder andere Malware bis hin zu unbefugtem Zugriff oder Hackingversuchen, fällt den Kollegen im Hauptquartier in Bologna zu. Sie arbeiten in der Regel aus der Ferne, außer bei Rennen im Heimatland oder einem Nachbarland. Die Kollegen vor Ort an der Rennstrecke befassen sich ausschließlich mit den Vorbereitungen rund um das Rennen. Aus diesem

ANFORDERUNGEN

Ducati Corse hat eine ganze Reihe von Anforderungen an die IT-Sicherheit. Es ist vor allem von größter Wichtigkeit, dass die Integrität der 20 Gigabyte an Renndaten, die während eines jeden Rennens gesammelt werden, gewahrt wird und die Daten vertraulich bleiben. Dazu gehören Sensordaten, die die Reaktion der Maschine auf verschiedene Parameter wie Beschleunigung, Stellung der Drosselklappen, ABS-Management, Reifendaten und einiges mehr abbilden. Diese Daten sind für das Team von Ducati Corse entscheidend bei der Planung für eine auf das Motorrad genau zugeschnittene Strategie. Diese Strategien sind das direkte Ergebnis des Mehrwerts, der durch die Kombination aus dem Talent der einzelnen Fahrer und der Expertise des Teams entsteht. Jede Ausnutzung einer Sicherheitslücke und jede Infektion mit Schadsoftware stellt ein ernstzunehmendes Risiko dar, welches zum Verlust einer ganz wesentlichen Firmenressource führen kann: der Verlust der Renndaten.



Insgesamt handelt es sich bei Ducatis mobilem Rechenzentrum um eine Infrastruktur, die mit Blick auf die Stabilität, die Zuverlässigkeit und den Schutz der Internetanbindung mit verschiedenen und teils schwierigen lokalen Bedingungen konfrontiert ist.

In einer Meisterschaft wie der MotoGP, in der jedes Team den Regeln gemäß eine identische Fahrzeugelektronik hat, kommt es im Rennen einzig auf die Rennstrategie sowie die Einstellung der individuellen Maschinen an. Die Aufgabe, sich um IT-Probleme zu kümmern, von

und anderen Gründen spielt die IT-Sicherheit eine wichtige Rolle für das Ducati-Team. Wie in jedem Unternehmen unterliegt die IT-Sicherheit auch bei Ducati Einschränkungen beim Budget und der Forderung nach einem Gleichgewicht zwischen Performance und Schutz. Die Leistungsfähigkeit der Systeme darf auf keinen Fall beeinträchtigt werden und auch die Reaktionsfähigkeit der Renntechniker muss in dieser Umgebung erhalten bleiben – schließlich muss das Team sicherstellen, dass die maximale Leistung abrufbar ist und Informationen schnell übertragen werden können.

Obwohl man vermuten könnte, dass gezielte Hackerangriffe die größte Bedrohung für das Ducati-Team sind, ist dieses Risiko tatsächlich zweitrangig: Ein externer Angreifer müsste im Vorfeld genau wissen, welche Art von Daten er erbeuten will. Ebenso müsste ein Angreifer wissen, wem er diese Daten zum Kauf anbieten kann, wodurch naturgemäß nur eine kleine Nische mit potenziellen Kunden übrigbleibt. Das Bedrohungspotenzial durch externe Angriffe, die sich in erster Linie gegen das Gäste-WLAN im Paddock richten und nicht gegen

„DER NIEDRIGE EINFLUSS AUF DIE SYSTEMLEISTUNG UND DAS LEVEL AN SICHERHEIT ERLAUBT HOHE ARBEITSLEISTUNGEN.“

Stefano Rendina, IT-Manager Ducati Corse

die Renn Daten, ist umgekehrt proportional zu Bedrohungen durch Insider: In einer Welt, in der eine starke Personalfuktuation herrscht, können aus Kollegen plötzlich Konkurrenten werden. Die Fahrer arbeiten gewohnheitsmäßig und aus einem gewissen Aberglauben heraus bevorzugt mit „ihren“ Mechanikern, Ingenieuren und Technikern zusammen. Aus diesem Grund ist die Ausstattung der Systeme mit einem wirksamen und proaktiven Schutz sowohl gegen interne als auch externe Bedrohungen eine besondere Herausforderung. Um diese Herausforderung zu meistern, setzt Ducati auf eine Sicherheitsstrategie, die sich auf mehrere Hersteller stützt. Nach ausführlichen Tests hat sich das Ducati-Team bei der Echzeitsicherung gegen Infektionen mit Schadsoftware für die G DATA Endpoint Protection Business entschieden.

G DATA Endpoint Protection Business



DIE LÖSUNG

G DATA Endpoint Protection schützt in Echtzeit die Integrität der wichtigsten Daten auf den Servern, die

bei der MotoGP eingesetzt werden und auf denen die Telemetriedaten gesammelt und aufgezeichnet werden. Die Wahl des Ducati-Teams fiel auf die G DATA Lösung, da sie ein hohes Maß an Flexibilität bietet und gleichzeitig einfach zu bedienen ist. Beides sind Schlüsselkriterien für eine Anwendung, die in einer leistungsoptimierten Umgebung wie der MotoGP zum Einsatz kommt. Mit zwei Scan-Engines, die die Umgebung nach Schadsoftware absuchen und der reibungslosen Integration der patentierten CloseGap-Technologie sorgt die G DATA Endpoint Protection für ein hohes Maß an Sicherheit im Vergleich zu Produkten, die nur eine Scan-Engine einsetzen. Gleichzeitig wird der Einfluss auf die Performance merklich reduziert.

„Die G DATA Lösung hat sich in dieser Hinsicht als wirkungsvoll erwiesen. Die MotoGP ist eine Marterstrecke, da die IT-Infrastruktur hohen Belastungen ausgesetzt ist und dabei zu jeder Zeit funktionieren und geschützt sein muss, egal wo auf der Welt und unter welchen Bedingungen am Rennort. Die G DATA Endpoint Protection zeigt sich dieser Herausforderung durch konstant hohe Erkennungsraten bei Schadsoftware und durch proaktives Reagieren gewachsen“, sagt Stefano Rendina, IT-Manager von Ducati Corse. „Der geringe Einfluss auf die Systemleistung und der hohe Grad an Schutzleistung erlaubt hohe Arbeitsleistungen ohne Verzögerungen bei der Analyse von Daten.“ In der neuesten Version der Software, die jedem Kunden mit einer gültigen Lizenz zur Verfügung steht, hat der deutsche Hersteller mit der Exploit

Protection eine weitere Schutztechnologie eingebaut, die wirksam vor Zero-Day-Bedrohungen schützt, bis eine verwundbare Anwendung vom Hersteller ein Update erhält.

Für die Verwaltung der Software hält die G DATA Endpoint Protection ein spezielles Dashboard bereit, mit dem ein Administrator sowohl eine Übersicht über den Clientstatus erhält, als auch eine Möglichkeit zur schnellen Einrichtung von Zugangsbeschränkungen – sogar aus der Ferne und in Echtzeit. Diese Echtzeitkontrolle ist ebenfalls eine der Grundvoraussetzungen von Ducati Corse. Einfaches und effizientes Policy Management hat sich vor allem während der ersten Rennen als wichtig erwiesen. „Die Festlegung von Zugriffsberechtigungen für bestimmte Dateiodner durch eine Sicherheitspolicy hat die unbefugten Zugriffe durch Insider um 20 - 30 % gesenkt“, fügt Rendina hinzu. Das IT-Team von Ducati arbeitet laufend an der Entwicklung weiterer Policies. Dieser Prozess geht mit dem Sammeln an Erfahrungen mit den Features, die G DATA bietet, einher; hier fließen auch die Erfahrungen aus dem Außeneinsatz ein. Beim ersten Ausrollen der Lösung auf den Rennsystemen, welche zu diesem Zeitpunkt in Qatar im Einsatz waren, wurde Rendina von einem Technikerteam von G DATA Italien begleitet. „Im Bedarfsfall Hilfe vor Ort zu haben, statt sich auf Mittelsleute verlassen zu müssen, die mit den örtlichen Gegebenheiten nicht vertraut sind, war ein weiterer einschlägiger Faktor, der zu unserer Entscheidung für die G DATA Endpoint Protection beigetragen hat.“

„DER SCHUTZ SOLCH KRITISCHER SYSTEME MIT EINER ZUVERLÄSSIGEN LÖSUNG IST NICHT DAS ZIEL, SONDERN DER AUSGANGSPUNKT.“

Stefano Rendina, IT-Manager Ducati Corse

SICHERHEIT WILL GETEILT WERDEN

Genau wie jedes andere kleine und mittelständische Unternehmen hat auch Ducati Corse kein unbeschränktes IT-Sicherheitsbudget. Rendina bestätigt: „Es ist wichtig, das obere Management so früh wie möglich in die Entscheidungsprozesse einzubinden. Damit kann sichergestellt werden, dass die Entscheidungsträger die Wichtigkeit der anstehenden Investition auf allen Ebenen nachvollziehen können und auch einen Einblick bekommen, welche Schäden potenziell durch Infektionen oder Datenverlust entstehen können.“

Es ist leicht, für mehr Sicherheit zu argumentieren, wenn dabei finanzielle Einbußen sowie der Verlust von Daten und Arbeitszeit im Vordergrund stehen. Ebenso wichtig ist es, alle verfügbaren Lösungen in Bezug auf ihre Eignung für die eigenen Budget-, Sicherheits- und Flexibilitätsanforderungen im Auge zu behalten. „Solch kritische Systeme mit einer zuverlässigen Lösung zu schützen, ist nicht das zu erreichende Ziel, son-



dern vielmehr ein Ausgangspunkt“, meint Rendina. „Sobald das Projekt anläuft, ist es genau so wichtig, dass die Anwender das Gefühl haben, in die Durchsetzung des Sicherheitskonzepts eingebunden zu sein. Betrachtet man den breiten Einsatz mobiler Endgeräte durch „nomadische“ Mitarbeiter und die Tatsache, dass es sich bei diesen Anwendern nicht unbedingt um IT-Spezialisten handelt, ist es ausschlaggebend, dass diese Mitarbeiter die Notwendigkeit sowohl einer Mobile Device

Management-Lösung erkennen, als auch der Nutzung von VPN-Tunneln zur Übermittlung von Daten zum/vom Hauptsitz oder zum Lesen von E-Mails.“

Ohne einen angemessenen Wissenstransfer können Projekte scheitern, bevor sie überhaupt richtig gestartet sind, weil und gerade wenn die Anwender deren Nutzen nicht erkennen.

WWW.GDATA.DE



**SIMPLY
SECURE**